

ATTACHMENT 2

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION**

CISCO SYSTEMS, INC.,

Plaintiff,

v.

ARISTA NETWORKS, INC.,

Defendant.

Case No. 5:14-cv-05344-BLF (PSG)

**OPENING EXPERT REPORT OF KEVIN ALMEROTH
REGARDING COPYING**

SUBMITTED ON BEHALF OF CISCO SYSTEMS, INC.

**CONTAINS HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY INFORMATION
AND SOURCE CODE**

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

32. I also have conducted research; co-authored papers; and developed systems to support the detection of plagiarism through document comparison and similarity detection (*see, e.g.*, the papers and systems in my CV, specifically II.A.55, II.A.40, II.B.36, and II.E.15). I have also used tools like CopyFind, PAIRwise, and the Measure of Software Similarity (MOSS) program in my courses.

33. Furthermore, I find programming an expressive, creative endeavor, just like technical writing. In both cases, although there is a purpose to be served, there are many ways to accomplish the goal, and a wide range of expressive choices in doing so.

34. I attach as **Attachment A** my *curriculum vitae*, which includes a more complete list of my qualifications.

B. Materials Considered

35. In forming my opinions, I have relied on my education and experience as described above.

36. I have also reviewed and considered the materials cited in this reports as well as the materials listed in **Attachment B** of this report, and the materials cited in all exhibits to this report, all of which are incorporated here by reference.

37. I also have inspected and/or tested:

- three Arista switches running EOS
- Arista’s EOS operating system produced by Arista in this litigation
- Arista’s EOS source code made available for inspection at the office of Arista’s counsel
- two Cisco switches running IOS (Catalyst 3560E, Catalyst 4948E)
- Cisco source code produced by Cisco in this litigation

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

- Source code relating to Stanford’s development of different technology

38. In addition to the materials specifically identified, I may provide further exhibits to be used as a summary of or support for my opinions.

39. I expect to testify at trial regarding the matters addressed in this report and any supplemental or amended report I may submit. I also expect to testify at trial with respect to matters addressed by experts testifying on behalf of Arista. I also may testify on other matters relevant to this case, if asked by the Court or by the parties’ counsel.

III. CISCO’S IOS PLATFORM

A. Technology Overview

40. The products involved in this case are network devices (routers and switches) and their operating systems and command line interface computer programs, including display inputs and outputs (“CLI”). Network devices are, at a high level, electronic devices that connect or create connections between one computer network and another and allow information to be transmitted among networks locally, regionally, nationally, and internationally. Network devices, for example, form the structural backbone of the Internet. They move or “forward” packets of data from the sender’s location to the recipient’s location along network pathways that can span the world. Individually, they determine the next hop towards a destination. Collectively, they determine the route that packets will take from a source to a destination. The science of routing and switching data through the Internet is complex and challenging because messages must be sent quickly, securely, and accurately; it is a science that is instrumental to the viability of the Internet and worldwide commerce.

41. Cisco has been the recognized world leader in internetworking technology since early in its history, including approximately when it began selling routers in the mid-1980s.

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

information from, the device. When a user enters a command, the device typically provides some type of feedback to the user, for example, command confirmation or the output of executing such a command.

51. In choosing to develop a CLI computer program (as opposed to other alternatives, *e.g.*, a graphical user interface), the Cisco engineers faced endless aesthetic choices for each of the numerous commands now found in the Cisco IOS CLI computer program and to select an elaborate structure and organization for these commands.⁸ Neither the commands nor the structure and organization of the commands were dictated by technical requirements—they could have comprised different letters or numbers and have been organized in various different number of ways.⁹ Additionally, Cisco designed expressive textual outputs that are used by the CLI computer program when providing feedback to the user and created an extensive set of command definitions as part of the program’s help system. Like the initial choice of a CLI computer program, each of these subsequent steps in the development of the program was guided by the creativity and personal preferences of Cisco’s engineers.¹⁰

52. The Cisco IOS CLI is the product of decades of investment and creative endeavor by Cisco. Cisco also has spent years developing comprehensive user documentation and user

⁸ Conversation with Kirk Lougheed (June 3, 2016); *see generally* Deposition Testimony of Kirk Lougheed; Abhay Roy; Adam Sweeney; Anthony Li; Devadas Patil; Greg Satz; Hugh Holbrook; Phillip Remaker; Ramanathan Kavasseri; and Tong Liu; *see also infra* Section V(C) (discussing creativity and originality).

⁹ Conversation with Kirk Lougheed (June 3, 2016); *see generally* Deposition Testimony of Kirk Lougheed; Abhay Roy; Adam Sweeney; Anthony Li; Devadas Patil; Greg Satz; Hugh Holbrook; Phillip Remaker; Ramanathan Kavasseri; and Tong Liu; *see also infra* Section V(C) (discussing creativity and originality).

¹⁰ *See generally* Deposition transcripts of Kirk Lougheed; Conversation with Kirk Lougheed (June 3, 2016); *see generally* Deposition Testimony of Kirk Lougheed; Abhay Roy; Adam Sweeney; Anthony Li; Devadas Patil; Greg Satz; Hugh Holbrook; Phillip Remaker; Ramanathan Kavasseri; and Tong Liu; *see also infra* Section V(C) (discussing creativity and originality).

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

(output for “show ip route”²⁴)

```

Spanning tree enabled protocol rstp
Root ID    Priority    32770
           Address    000d.eca3.9f01
           Cost       4
           Port       4105 (port-channel10)
           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID  Priority    32770 (priority 32768 sys-id-ext 2)
           Address    0022.5579.7641
           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interface      Role Sts Cost      Prio.Nbr Type
-----
Po10           Root FWD 2         128.4105 (vPC peer-link) P2p
Po20           Desg FWD 1         128.4115 (vPC) P2p
Po30           Root FWD 1         128.4125 (vPC) P2p

```

(output for “spanning tree enabled protocol rstp”²⁵)

65. CLI screen outputs are a key part of the IOS CLI “look and feel” as they are the expressions that a user (typically a network engineer) interacts with and is able to respond to. And it is one of the distinct ways that a user knows that he or she is using Cisco’s IOS CLI. As with the command inputs, the Cisco engineers faced endless aesthetic choices for each of the numerous screen outputs now found in the Cisco IOS CLI computer program. The structure and organization of the screen outputs were not dictated by technical requirements—they could be been organized in various different number of ways.

F. IOS-XR

66. IOS XR is a series of Cisco IOS versions used on carrier-grade routers such as the CRS series, 12000 series, and ASR9000 series. IOS-XR was designed to service the needs of

²⁴ CSI-CLI-00248571, Cisco IOS Asynchronous Transfer Mode Command Reference (2011), at 476.

²⁵ CSI-CLI-00178252, Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2013), at 63.

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

Cisco Nexus 2000 Series Fabric Extenders; Cisco MDS 9000 Family storage switches; and Cisco UCS 6100 Series Fabric Interconnects.²⁸

IV. ARISTA’S EOS PLATFORM

A. EOS Overview

69. Founded in 2004 by former Cisco engineers, Arista Networks (“Arista”) is one of Cisco’s competitors in the internetworking industry. According to Arista’s CEO—a former Cisco executive—Cisco is viewed by Arista as a “fierce competitor.”²⁹ Like Cisco, Arista sells switches with an operating system and command line interface computer program, referred to by Arista as the Extensible Operating System (“EOS”). According to Arista, its EOS “is the core of Arista cloud networking solutions for next-generation data centers and cloud networks.”³⁰ The switches that Arista’s sells with its EOS and CLI are based on 10GbE, 40GbE, and 100GbE platforms, and include at least its 7010T, 7280SE, 7150S, 7050TX, 7050SC, 7050OX, 7250OX, 7060CX, 7260X, 7300 series, and 7500R series switches.

70. As the evidence below shows, Arista’s purpose in creating EOS was to create a substitute for Cisco’s IOS. EOS directly competes with IOS in the market such that if a competitor has an Arista switch running EOS they have no need for Cisco switches running IOS (or one of Cisco’s other copyrighted operating systems).

²⁸ See http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/nx-os-software/data_sheet_c78-652063.pdf; Cisco copyrighted documentation submitted with the Copyright Office for this operating system as set forth in Cisco’s responses to Interrogatory Nos. 24 and 25, which are incorporated here by reference.

²⁹ CSI-CLI-00357842 at CSI-CLI-00357851.

³⁰ See <https://www.arista.com/en/products/eos>.

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

Arista Operational Similarities/Differences

- **Similarities**

- Industry standard "IOS like" CLI
- L2/L3 protocol standards support
- Standard operational protocols support (SNMP, syslog, etc)

[REDACTED]

³² ANI-ITC-944_945-3473603.

³³ ARISTANDCA1195413 (emphasis added).

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

75. As Arista’s own executives and engineers also have explained to the public, the EOS CLI was intentionally designed to be similar to Cisco’s IOS CLI:

- “[A] Cisco CCIE expert would be able to use Arista right away, because we have a similar command-line interface and operational look and feel. Where we don’t have to invent, we don’t.”³⁵
- Arista tried to “[p]rovide familiar interfaces to ease adoption” including a “standard CLI that ... retains familiar management commands” such that “80% [of Arista customers] tell [Arista] they appreciate the way they can leverage their deep [Cisco] IOS experience, as they can easily upgrade an aging [Cisco] Catalyst infrastructure to Arista.”³⁶
- “Familiar management interfaces, standard CLI ... It’s been very helpful for our customers to be able to rapidly adopt our products and integrate them into their environments ... that our switches provide a familiar management interface so their existing tools and processes, screen scraping, automation, continue to work just as they did before.”³⁷

76. Many other examples of Arista employees confirming that the EOS CLI was designed to be similar to Cisco’s IOS CLI are discussed below.³⁸

³⁴ ANI-ITC-944_94 0962624 at ANI-ITC-944_945-0962625.

³⁵ CSI-ANI-00381280, John Gallant, “How Arista Networks Got Out In Front of the SDN Craze,” Network World (Feb. 22, 2013).

³⁶ Posting of Kenneth Duda to Arista EOS Central, “Linux as a Switch Operating System: Five Lessons Learned” (Nov. 5, 2013), *available at* <https://eos.arista.com/linux-as-a-switch-operating-system-five-lessons-learned/>.

³⁷ Arista, *EOS Bits & Bytes - Episode 1 - Lessons Learned While Building a Network OS on Top of Linux*, Arista EOS Central - Video Library (Jan. 30, 2014), at 6:55–7:56, *available at* <http://eos.arista.com/wpcontent/themes/aristaeos/video-lightbox.php?vid=ttp6lavHKGo>.

³⁸ See *infra* Section VI(A).

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

77. Like Cisco, Arista has documentation related to its EOS platform as well as the EOS CLI.³⁹ Arista’s documentation describes the command syntax, structure, modes, prompts, and related information sufficient to teach a user how to operate Arista’s EOS CLI.⁴⁰

■ [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

■ [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

³⁹ See generally CSI-CLI-00007473, CSI-CLI-00007244, CSI-CLI-00006858, CSI-CLI-00007841, CSI-CLI-00010517, CSI-CLI-00008985, CSI-CLI-00014141, CSI-CLI-00011973, CSI-CLI-00018146, CSI-CLI-00000084, CSI-CLI-00004616, CSI-CLI-00020575, CSI-CLI-00002332, CSI-CLI-00016001.

⁴⁰ *Id.*

■ [REDACTED]

■ [REDACTED]

■ [REDACTED]

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

[REDACTED]

80. As part of preparing this report, I also performed extensive testing on Arista’s EOS CLI. I have provided exemplary images of a computer screen showing the CLI display that an Arista customer would see when it logs into an Arista switch running EOS:

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

```

Arista Networks EOS 4.14.9.1M
localhost login:

Abboot 3.0.3-1262453

Press Control-C now to enter Abboot shell
Booting flash:EOS-4.14.5.1F-SSU.swi
[ 9.586323] Starting new kernel
Switching rootfs

Welcome to Arista Networks EOS 4.14.5.1F-SSU
Mounting filesystems: [ OK ]
Starting udev: [ OK ]
Setting hostname localhost: [ OK ]
Entering non-interactive startup
Starting ProcMgr: [ OK ]
Starting EOS initialization stage 1: [ OK ]
ip6tables: Applying firewall rules: [ OK ]
iptables: Applying firewall rules: [ OK ]
iptables: Loading additional modules: nf_conntrack_tftp [ OK ]
Starting system logger: [ OK ]
Starting NorCal initialization: [ OK ]
Retrigger failed udev events[ OK ]
Starting isshd: [ OK ]
Starting mcelog daemon
Starting EOS initialization stage 2: [ OK ]
Starting Power On Self Test (POST): [ OK ]
Starting crond: [ OK ]
Completing EOS initialization (press ESC to skip): [ OK ]
Model: DCS-7500E-SUP
Serial Number: JPE14211632
System RAM: 16012348 kB
Flash Memory size: 3.4G

localhost login: █

```

(Arista DCS-7554 running EOS 4.14.5.1F-SSU)

C. EOS Program

81. In order to understand and analyze Arista’s EOS, I have reviewed its programs on numerous occasions.

82. Arista’s EOS program provides the EOS CLI and contains specific programs and functions. For example, EOS includes programs to generate a command line interface and

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

command line into which commands can be entered (as shown above). EOS (like Cisco’s IOS) is able to execute entered commands (including the 500+ multi-word command expressions asserted in this case) within the construct of specific hierarchical modes and sub-modes,⁴⁵ as explained in Arista’s user manuals and guides as well.⁴⁶

3.4 Command Modes

Command modes define the user interface state. Each mode is associated with commands that perform a specific set of network configuration and monitoring tasks.

- Section 3.4.1: Mode Types lists the available modes.
- Section 3.4.2: Navigating Through Command Modes lists mode entry and exit commands.
- Section 3.4.3: Command Mode Hierarchy describes the mode structure.
- Section 3.4.4: Group-Change Configuration Modes describes editing aspects of these modes.

3.4.1 Mode Types

The switch includes these command modes:

- **EXEC:** EXEC mode commands display system information, perform basic tests, connect to remote devices, and change terminal settings. When logging into EOS, you enter EXEC mode.

EXEC mode prompt: `switch>`

- **Privileged EXEC:** Privileged EXEC mode commands configure operating and global parameters. The list of Privileged EXEC commands is a superset of the EXEC command set. You can configure EOS to require password access to enter Privileged EXEC from EXEC mode.

Privileged EXEC mode prompt: `switch#`

- **Global Configuration:** Global Configuration mode commands configure features that affect the entire system, such as system time or the switch name.

Global Configuration mode prompt: `switch(config)#`

- **Interface Configuration:** Interface configuration mode commands configure or enable Ethernet, VLAN, and Port-Channel interface features.

Interface Configuration mode prompt: `switch(config-if-Et24)#`

- *Protocol specific mode:* Protocol specific mode commands modify global protocol settings. Protocol specific mode examples include **ACL Configuration** and **Router BGP Configuration**.

The prompt indicates the active command mode. For example, the Router BGP command prompt is `switch(config-router-bgp)#`

⁴⁵ Mode Hierarchy: Mode CliParser.py > ConfigModeBase BasicCli.py > GlobalConfigMode BasicCli.py.

⁴⁶ CSI-CLI-00016001 at CSI-CLI-00016113; *see also* ANI-ITC-944 _ 945-0962624 at ANI-ITC-944 945-0962628 (“Multiple levels of modes are OK, too. Our support for these is improving, and they help to identify the objects being configured in the naturally nested structure of many configuration models.”).

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

[illegible]

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

[REDACTED]

[REDACTED]

[REDACTED]

87. As explained below, Arista’s EOS also includes hundreds of textual similarities as compared to Cisco’s IOS, including hundreds of command descriptions.

V. THE COPYRIGHTED WORKS

A. My Understanding Of Certain Legal Principles

88. I have been informed that under the law, a copyright owner has the exclusive right to do and to authorize others to reproduce, prepare derivative works from, distribute, publicly perform, or publicly display, the copyrighted work. I understand that the term derivative work refers to a work based on one or more preexisting works, including a work in which the preexisting work or works is/are recast, transformed, or adapted.

89. It is my understanding that to establish direct copyright infringement, a plaintiff must prove that the plaintiff is the owner of the copyright and that the defendant copied elements of the copyrighted work.

90. I understand that one way to prove that the defendant copied the plaintiff’s work, the plaintiff may show that the defendant had access to the plaintiff’s copyrighted work and that there are similarities between the defendant’s work and the plaintiff’s work.

91. I further understand that in assessing similarity, courts consider both quantitative similarity—how much was copied—as well as qualitative similarity—the significance of what was copied.

⁴⁷ When a CliPlugin defines a new command, the method `Mode.addCommand()` in `CliParser.py` (`Mode` in `CliParser.py`) is invoked.

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

	CSI-CLI-00356490 - CSI-CLI-00356495	CSI-CLI-00356506 - CSI-CLI-00356507	(supplementing TXu-1-036- 066)		
Cisco IOS 12.2	CSI-CLI-00356508 - CSI-CLI-00356511 CSI-CLI-00356556 - CSI-CLI-00356561	CSI-CLI-00356506 - CSI-CLI-00356508 CSI-CLI-00356536 - CSI-CLI-00356537	TXu-1-057- 806 (supplementing TXu-1-036- 065)	5/2001	6/14/2002
Cisco IOS 12.3	CSI-CLI-00356524 - CSI-CLI-00356527	CSI-CLI-00356542 - CSI-CLI-00356545	TXu-1-188- 975	Summer 2003	7/26/2004
Cisco IOS 12.4	CSI-CLI-00356486 - CSI-CLI-00356489	CSI-CLI-00356705 - CSI-CLI-00356705	TXu-1-259- 162	5/2/2005	8/12/2005
Cisco IOS 15.0	CSI-CLI-00356480 - CSI-CLI-00356483	CSI-CLI-00356564 - CSI-CLI-00356567	TX 7-938-524	10/1/2009	11/28/2014
Cisco IOS 15.1	CSI-CLI-00356502 - CSI-CLI-00356505	CSI-CLI-00356532 - CSI-CLI-00356535	TX 7-938-525	3/26/2010	11/28/2014
Cisco IOS 15.2	CSI-CLI-00356528 - CSI-CLI-00356531	CSI-CLI-00356697 - CSI-CLI-00356700	TX 7-937-159	7/22/2011	11/24/2014
Cisco IOS 15.4	CSI-CLI-00356657 - CSI-CLI-00356660	CSI-CLI-00356653 - CSI-CLI-00356656	TX 7-938-341	11/24/2013	11/26/2014
Cisco IOS XR version 3.0	CSI-CLI-00356665 - CSI-CLI-00356668	CSI-CLI-00356618 - CSI-CLI-00356621	TXu-1-237- 896	2004	4/29/2005
Cisco IOS XR version 3.2	CSI-CLI-00356661 - CSI-CLI-00356664	CSI-CLI-00356701 - CSI-CLI-00356704	TXu-1-270- 592	2005	10/19/2005
Cisco IOS XR version 3.3	CSI-CLI-00356689 - CSI-CLI-00356692	CSI-CLI-00356642 - CSI-CLI-00356645	TXu-1-336- 997	2006	7/19/2006
Cisco IOS XR version 3.4	CSI-CLI-00356634 - CSI-CLI-00356637	CSI-CLI-00356638 - CSI-CLI-00356641	TXu-1-344- 750	2006	3/2/2007
Cisco IOS XR version 3.5	CSI-CLI-00356685 - CSI-CLI-00356688	CSI-CLI-00356614 - CSI-CLI-00356617	TXu-1-592- 305	2007	7/17/2007
Cisco IOS XR version 4.3	CSI-CLI-00356681 - CSI-CLI-00356684	CSI-CLI-00356649 - CSI-CLI-00356652	TX 7-933-364	12/21/2012	11/14/2014
Cisco IOS XR version 5.2	CSI-CLI-00356626 - CSI-CLI-00356629	CSI-CLI-00356602 - CSI-CLI-00356605	TX 7-933-353	7/5/2014	11/14/2014
Cisco IOS XE version 2.1	CSI-CLI-00356693 - CSI-CLI-00356696	CSI-CLI-00356606 - CSI-CLI-00356609	TX 7-937-240	5/2/2008	11/24/2014
Cisco IOS XE version 3.5	CSI-CLI-00356610 - CSI-CLI-00356613	CSI-CLI-00356630 - CSI-CLI-00356633	TX 7-937-234	11/28/2011	11/24/2014
Cisco NX-OS Release 4.0	CSI-CLI-00356646 - CSI-CLI-00356648	CSI-CLI-00356622 - CSI-CLI-00356625	TX 7-940-713	4/2/2008	11/13/2014
Cisco NX-OS Release 5.0	CSI-CLI-00356599 - CSI-CLI-00356601	CSI-CLI-00356677 - CSI-CLI-00356680	TX 7-940-718	5/24/2010	11/13/2014
Cisco NX-OS Release 5.2	CSI-CLI-00356596 - CSI-CLI-00356598	CSI-CLI-00356673 - CSI-CLI-00356676	TX 7-940-727	7/29/2011	11/13/2014
Cisco NX-OS Release 6.2	CSI-CLI-00356593 - CSI-CLI-00356595	CSI-CLI-00356669 - CSI-CLI-00356672	TX 7-940-722	8/22/2013	11/13/2014

98. Much of the IOS-related programs, documentation, and other materials that I reviewed in preparing this report bear Cisco copyright notices, making it apparent that Cisco owns the copyrights to these materials.

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

C. Copyrightable Expressions in Cisco’s CLI: Originality & Creativity

99. I understand that Cisco contends that hundreds of multi-word command expressions have been copied by Arista.⁴⁸ I also understand that Cisco contends that Arista copied the associated command modes, prompts, as well as the following command hierarchies:

- “aaa” command hierarchy
- “bgp” command hierarchy
- “clear” command hierarchy
- “dot1x” command hierarchy
- “ip” command hierarchy
- “ipv6” command hierarchy
- “neighbor” command hierarchy
- “show” command hierarchy
- “snmp-server” command hierarchy
- “spanning-tree” command hierarchy
- “vrrp” command hierarchy

100. I also understand that Cisco contends that original documentation such as user manuals and screen outputs relating to its copyrighted works have also been copied as well as command descriptions (also known as help descriptions, help screens, or “helpdesc”).

101. It is my opinion that Cisco’s asserted command expressions, hierarchies, modes, and prompts contain considerable original expression in their selection and arrangement. To start, designing a command syntax for a particular function is a subjective exercise that requires independent judgment of the author and numerous creative and expressive choices. For example, an author must select one or more individual words that she wants to use. The author must then determine the spelling of those words and whether to abbreviate or otherwise modify the traditional spelling. The author must determine what order to place the words in and the relationship, if any, that the words should have with one another. All of those decisions are left to the subjective judgement and creativity of the command author. In some respect, any one of

⁴⁸ See Exhibit 1 to Cisco’s Second Amended Complaint.

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

the asserted command expressions could, in theory, be any random set of words or characters, and yet the command would still work. Choosing the words and the arrangement and the organization of those words is where the creativity lies.

102. My opinions are supported by sworn testimony of both Cisco and Arista. For example, Cisco distinguished engineer and IOS CLI creator Kirk Lougheed testified that as a general matter creating a piece of software is a creative process:⁴⁹

24 THE WITNESS: Writing any piece of
 25 software involves some degree of creativity. It may
 1 not be at the Shakespearean level, but maybe more
 2 prosaic. But you actually have to figure out
 3 something. You have to create something to show how
 4 stuff is done or to create something to communicate.
 5 And that’s what I was doing was creating something
 6 to communicate to the customer, to the user of the
 7 stuff, here is a command expression that will get
 8 you information, and it’s easy enough to understand
 9 what was being done.

103. Mr. Lougheed also explained that crafting commands themselves is a creative process and that specific command expressions may change during that process based on the aesthetic sensibilities and subjective judgment of the author:⁵⁰

10 Q Did you come up with the phrase “IP
 11 address”?

 3 It became clear that much more—that we
 4 were becoming a multi-protocol router. We were
 5 adding other protocols into the box, into the
 6 software.
 7 And I had—I value—I value the
 8 aesthetic of having a symmetric-looking command line
 9 expression, symmetric hierarchy. It was clear we
 10 were heading towards a hierarchy.
 11 So at some point after DECnet and perhaps

⁴⁹ Deposition Testimony of Kirk Lougheed Tr. at 338:24-339:9 (Apr. 4, 2016).

⁵⁰ Deposition Testimony of Kirk Lougheed Tr. at 128:10-129:19 (Nov. 20, 2015).

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

12 a few other protocols to make things look very
 13 similar, we started prefacing our IP-only commands
 14 with “IP.” And that gave a very—what I thought
 15 was a very elegant, symmetric, elegant way of
 16 referring to different protocols within a
 17 multi-protocol router.
 18 So that is the history of the “IP address”
 19 command.

104. Mr. Lougheed provided similar testimony for specific multi-word command expressions as well such as “show ip route,”⁵¹ “show spanning-tree,”⁵² “IP routing,”⁵³ “show hosts,”⁵⁴ “clear” hierarchy,⁵⁵ and “timers basic RIP.”⁵⁶

105. Another Cisco CLI command author, Mr. Abhay Roy, testified similarly. For instance, Mr. Roy testified that the creation of the command “bfd all-interfaces” was the result of looking at a variety of protocols, collectively discussing the best way to express the concept, considering how the command “fits into the bigger ... pieces of organization of commands, what makes sense, [and] what is more aesthetically correct” within the framework of the system.⁵⁷ Mr. Roy also testified he considered many things when designing commands such as content, features, “what is being asked,” and that during the creative process “you start with your best

⁵¹ Deposition Testimony of Kirk Lougheed Tr. at 331:6-23 (April 4, 2016).

⁵² *Id.* at 337:17-20.

⁵³ Deposition Testimony of Kirk Lougheed Tr. at 145:3-25 (Nov. 20, 2015).

⁵⁴ *Id.* at 168:21-169:16 (testifying that there were other command word options he could have chosen including “computers,” “names,” “systems,” “network systems,” “end systems”).

⁵⁵ *Id.* at 174:5-175:4 (“it seemed aesthetically pleasing to me”).

⁵⁶ *Id.* at 185:13-186:5.

⁵⁷ Roy Deposition Tr. at 24:12-25; 26:2-9 (discussing that command creation involves considering “overall architecture purity”); 45:6-20 (testifying that when creating commands Cisco wanted to make “smart choices” that made sense from an “aesthetic perspective” and from “the alignment and architectural perspective”).

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

guess,” which “may or may not be the best which will eventually have the light of day, but you go with your knowledge and your judgment.”⁵⁸

106. Another Cisco CLI command author, Mr. Devadas Patil, testified that the command creation process is subjective and implicates various considerations that are open to an author’s own professional judgment:

- “Well, there is—the—the product owner, which is me, lead developer for the product, comes up with initial proposal, and it is, essentially, reviewed by a group of people that are highly experienced for—for usability and extensibility, and so on, so there are certain criteria that they look—look at, including usability, extensibility, aesthetics, etc.”⁵⁹
- “So there’s a—there’s a—there’s a balance between future-proofing and—and verbosity, and—and the more you try to feature proof, the more verbose you can become, so it’s more of a subjective column how you design, keeping all of these in mind, yeah.”⁶⁰
- “Yeah, so intuitiveness, extensibility, usability, aesthetics are all factors that we considered.”⁶¹

107. Cisco engineer and CLI author Phillip Remaker’s testimony confirms the same. Mr. Remaker testified that commands, *e.g.*, “show inventory,” were created at Cisco through a collective discussion with other engineers (sometimes referred to as the Cisco “Parser Police”) during which many different word choices were considered:⁶²

2 Q. In your view, what’s creative about the
3 command “show inventory”? Strike that.
4 What is creative about the command “show
5 inventory”?
6 MR. NEUKOM: Objection. Calls for a legal
7 conclusion and personal opinion. Also off topic.
8 THE WITNESS: For this particular command,
9 we spent a lot of time in discussion and considered

⁵⁸ *Id.* at 47:8-18.

⁵⁹ Patil Deposition Tr. at 161:19-162:1 (Feb. 21, 2016).

⁶⁰ *Id.* at 186:7-11.

⁶¹ *Id.* at 187:1-9.

⁶² Remaker Deposition Tr. at 114:2-15 (Mar. 31, 2016).

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

10 a lot of different ideas for how to go about doing
 11 this command. And because we engaged a number of
 12 people and spent a lot of serious time thinking
 13 about the problem and how the customer would
 14 interact with the command, I think that careful
 15 consideration could be classified as creativity.

108. Communications from other Cisco engineers further confirm that the process of command expression creation is a subjective, creative endeavor. For example:

- Adam Sweeney (formerly of Cisco, now with Arista): “I agree with CLI naming is very subjective. . . . Review in this list gives us a chance to work towards consistency within this very subjective space.”⁶³
- Scott Lennartz (Cisco): “It is my belief that any exercise in naming is highly subjective, and there is rarely a ‘right’ answer”⁶⁴

109. This collaborative, creative, expressive process is what ultimately led to the Cisco command syntax of Cisco’s IOS CLI and “an aesthetic of the organization of the commands,” which includes the “hierarchical notions, the modality, the organization of the commands, and the choices of the words.”⁶⁵ And, as Mr. Remaker testified, one of the reasons why Cisco chose to organize commands into hierarchies was to “improve[] the readability of configurations.”⁶⁶ In other words: “Instead of having a single configuration line with a lot of attributes, it makes more sense to have individual lines expressing each individual attribute.”⁶⁷

⁶³ CSI-CLI00608716.

⁶⁴ CSI-CLI00608716.

⁶⁵ Remaker Deposition Tr. at 98:22-99:12 (Mar. 30, 2016).

⁶⁶ *Id.* at 106:25-107:5.

⁶⁷ *Id.* at 107:7-12.

111. By way of example, the command “show” is an expression of the idea or concept of displaying a particular configuration status of the device. There are many different ways to implement that idea and many different ways to even express that idea. For example, the word “display,” “print,” “watch,” “view,” or “info” are equally sufficient ways to express this idea. Other words such as “steve” or “book” or “phone” would be used just as well—a computer can recognize any combination of letters and numbers. Indeed, other vendors—such as Huawei—implement a command hierarchy using the command “display” instead of “show.”

[illegible]

46

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

[illegible]

[REDACTED]

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

[REDACTED]

[REDACTED]

[REDACTED]

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

[illegible]

[illegible]

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] [REDACTED]

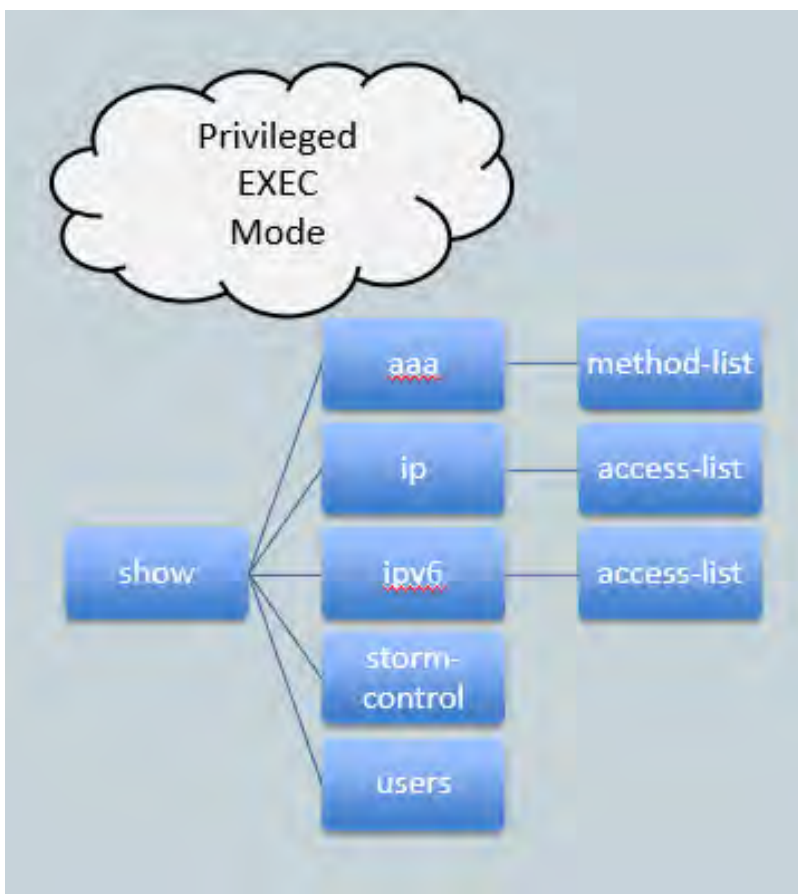
[illegible]

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE



113. The copied command hierarchies also contain considerable original expression. The decision to organize Cisco’s IOS CLI commands into the designers’ chosen hierarchy reflects the original choices of the designers. As an illustration, a sub-command hierarchy for “show” in Privileged EXEC mode is diagrammed below:

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE



114. Through this particular design, the designers were able to convey that a specific set of second words or tokens would follow the initial token, and then a further set, etc. The hierarchy conveys to a user an aesthetic sense of the set of choices, *i.e.*, what is possible and what is not. In some cases (*e.g.*, the use of “access-list” as an option under multiple higher level tokens), the hierarchy helps to organize choices into parallel possibilities.

115. By branching initially on the dimension of “show” and then building out the hierarchy from there, the designers created an organizational structural that is aesthetically pleasing, easy to understand, and easier to remember (based on the subjective belief and professional judgment of Cisco’s designers). A computer can execute the command “show_aaa_method-list” just as easily as it can execute a command called

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

“show_command_ipv6_access-list.” The reason for choosing the organizational structure in the way that Cisco’s designers did is so that they would have a unique command structure that Cisco’s customers would easily be taught (again, based on the subjective belief and professional judgment of Cisco’s designers) and because there was value in “the aesthetic of having a ... symmetric hierarchy” that was “elegant.”⁶⁹

116. The decisions to organize Cisco’s commands into modes with specific prompts reflects yet another conscious choice of expression. The command modes that I understand Cisco to be asserting in this case include “EXEC,” “Privileged EXEC,” “Global configuration,” and “Interface configuration” (collectively, the “asserted command modes”). Rather than placing commands into different modes with unique prompts, the designers could have created a unified command structure without different modes and chosen a single prompt. Alternatively, Cisco’s designers could have used different names for the asserted modes; for example, they could have chosen “ADMIN” instead of “EXEC” or “Secure ADMIN” instead of “Privileged EXEC.” Similarly, “Universal setup” could have been chosen instead of “Global configuration” or “Edge setup” instead of “Interface configuration.” Almost any other word choice could have been selected.

117. Further evidence that elements of Cisco’s IOS CLI are creative is that they are what the user sees, what the user knows, and how the user talks to and interacts with the Cisco device. The user interface defines the user’s experience. With the right selection of unique, intuitive commands and hierarchies—which Cisco endeavored to create on its own—Cisco built a successful business and became a market leader. That makes Cisco’s IOS CLI distinctive compared to other competitors.

⁶⁹ Deposition Testimony of Kirk Loughheed Tr. at 128:10-129:19 (Nov. 20, 2015).

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
[REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

- [REDACTED]
- [REDACTED]

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

134. The following independent forms of copying are covered by this report: (i) Arista’s copying of copyrighted expressions in programs (including CLI commands, modes, hierarchies, prompts and screen outputs) from Cisco’s copyrighted works into both physical and electronic media; (ii) Arista’s copying of copyrighted expressions in documents from Cisco’s copyrighted works into both physical and electronic media; and (iii) Arista’s copying of copyrighted expressions in screen displays from Cisco’s copyrighted works into both physical and electronic media. I understand that each one of these forms of copying are, alone, sufficient to establish copyright infringement.

A. Arista Had Access To Cisco’s Copyrighted Works & Admitted Copying

135. Arista had access to Cisco’s copyrighted works through a variety of sources, and, based on my inspection of the testimony and documents available in this case, it is my opinion that Arista has copied Cisco’s copyrighted expressions in its IOS copyrighted works.

136. Generally, Cisco’s copyrighted documents such as its IOS-related manuals have been available to the public and on Cisco’s website for years. Much of the Cisco documentation that I have personally observed contained a Cisco copyright notice, for example:



(IOS 11.0 (1989-1997), CSI-CLI-00430706)

Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Software Configuration Guide
© 2008 Cisco Systems, Inc. All rights reserved.

(IOS-XE 2.1 (2008), CSI-CLI-00229755)

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

Text Part Number: OL-5903-04

(IOS-XR 3.2 (2005), CSI-CLI-00362851)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2008 Cisco Systems, Inc. All rights reserved.

(NX-OS 4.0 (2008), CSI-CLI-00362851)

137. Cisco’s products incorporating the IOS CLI copyrighted works have been and are publicly available as well (some well before the founding of Arista), and the Cisco operating systems that I inspected running on Cisco devices all have copyright notices on them. Therefore, anyone who sees IOS running or the related documentation is aware (or should be aware) that Cisco has legal rights associated with IOS and its related materials.

■ [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

■ [REDACTED]

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[REDACTED] [REDACTED] [REDACTED]

[REDACTED]

Network Resources

Here is a table of some things on the internal network that can be useful to get your work done.

Resource	How to access	Notes
Arastra Internal Web	http://aweb	Everything that we've automated internally.
AID server	http://aid	Arastra Internal Documents available on line.
Bugzilla	http://bugs	Our bug database.
Proglog	http://proglog	You can view or update logs people have created of what they've been working on.
Autobuild report	http://abuild	Indications of whether your project's autobuild is working or not, and if not, who is working on fixing things.
Benchmark report	http://benchmark	Historical records of our benchmarks (performance tests), viewable via your web browser.
cisco806	telnet cisco806	A real-life Cisco 806, which is a branch office VPN gateway. You can learn about the IOS CLI, logging, and general device behavior. The device is physically located on kduda's desk. All relevant usernames and passwords are "arastra".

[REDACTED] [REDACTED]

[REDACTED] [REDACTED]

[REDACTED] [REDACTED]

[REDACTED] [REDACTED]

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

```
cisco3560>show parser dump config-vlan
Mode Name :config-vlan
```

```
1 name <string>
1 exit
1 mtu <576-18190>
1 state active
1 state suspend
1 said <1-4294967294>
1 media ethernet
1 media fddi
1 media tokenring
1 media fd-net
1 media tr-net
1 bridge type
1 bridge
1 bridge <0-15>
...
```

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

work for while employed at Cisco and characterizes these employees as “Arista Competitive Experts.”⁹⁰

143. Many of Arista’s engineers and executives are former Cisco employees. For example, Arista’s CEO Jayshree Ullal—who initially “made her career at ... Cisco Systems”—stated the following in an interview with Forbes magazine: “Since I helped build the enterprise, I would never compete with Cisco directly in the enterprise in a conventional way. It makes no sense. It would take me 15 years and 15,000 engineers, and that’s not a recipe for success.”⁹¹ Other former Cisco employees who are or have been members of Arista’s executive team and/or vice presidents include Andy Bechtolsheim, Anshul Sadana, Kenneth Duda, Isabelle Bertin-Bailly, Ed Chapman, Mark Foss, Christophe Metivier, Jeffrey Hirschman, Hugh Hollbrok, Jeff Raymond and Adam Sweeney, among others.

144. And in order for Arista customers to configure and use Arista’s products, Arista requires them to use the commands that Arista built into its system, which means that Arista’s customers also have access to Cisco’s IOS copyrighted works to the extent that Arista incorporated those works into its products.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

⁹⁰ Deposition of Sadana (Rough) Tr. at 75:15-77:9 (May 27, 2016); *see also* Sadana Exhibit 1303.

⁹¹ *See, e.g.*, CSI-ANI-00356028, Adam Lashinsky, “An Ex-Cisco Exec Reflects,” *Fortune* (Mar. 20, 2014), *available at* <http://fortune.com/2014/03/20/an-ex-ciscoexec-reflects/>.

⁹² [REDACTED]

[REDACTED]

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

- “[A] Cisco CCIE expert would be able to use Arista right away, because we have a similar command-line interface and operational look and feel. Where we don’t have to invent, we don’t.”⁹³
- Arista has tried to “[p]rovide familiar interfaces to ease adoption” including a “standard CLI that ... retains familiar management commands” such that “80% [of Arista customers] tell [Arista] they appreciate the way they can leverage their deep [Cisco] IOS experience, as they can easily upgrade an aging [Cisco] Catalyst infrastructure to Arista.”⁹⁴
- “Familiar management interfaces, standard CLI ... It’s been very helpful for our customers to be able to rapidly adopt our products and integrate them into their environments ... that our switches provide a familiar management interface so their existing tools and processes, screen scraping, automation, continue to work just as they did before.”⁹⁵
- “The familiar EOS command-line interface (CLI) avoids retraining costs.”⁹⁶

146. Arista’s CTO Kenneth Duda also admitted during a recorded interview that Arista “slavishly” copied Cisco:

- “We want to minimize the transition costs to our customers. Our customers come very well trained, big staffs of people who understand that—that particular CLI. We actually copied it slavishly. You know it’s like—even the things we thought were really silly, we went ahead and copied them anyway”⁹⁷

⁹³ CSI-ANI-00381280, John Gallant, “How Arista Networks Got Out In Front of the SDN Craze,” Network World (Feb. 22, 2013).

⁹⁴ Posting of Kenneth Duda to Arista EOS Central, “Linux as a Switch Operating System: Five Lessons Learned” (Nov. 5, 2013), *available at* <https://eos.arista.com/linux-as-a-switch-operating-system-five-lessons-learned/>.

⁹⁵ Arista, *EOS Bits & Bytes - Episode 1 - Lessons Learned While Building a Network OS on Top of Linux*, Arista EOS Central - Video Library (Jan. 30, 2014), at 6:55–7:56, *available at* <http://eos.arista.com/wpcontent/themes/aristaeos/video-lightbox.php?vid=ttp6lavHKGo>.

⁹⁶ Arista, *EOS: An Extensible Operating System*.

⁹⁷ Packet Pushers Clip (Audio File) (Duda Exh. 274).

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[illegible]

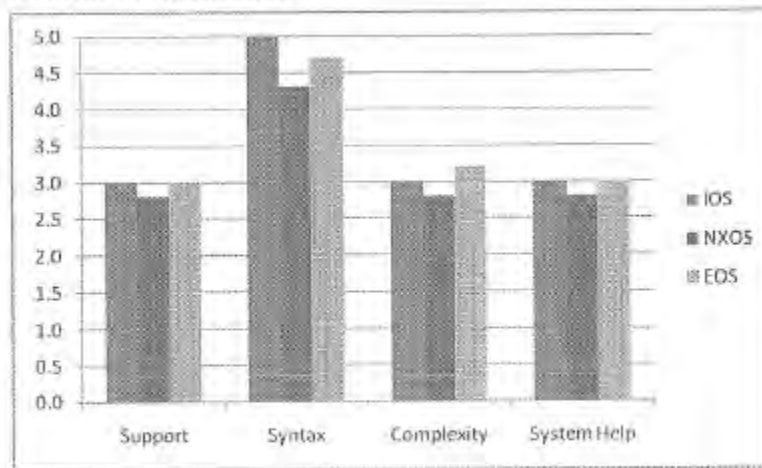
[REDACTED]

[REDACTED] [REDACTED]

[REDACTED] [REDACTED]

[illegible]

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

Overall Performance

Commentary: Overall, success in adjustment is a factor of how well the platform meets or exceeds the behavior expected by the IOS user. Both platforms performed well, and the tests showed that the level of adjustment for an IOS platform to either would be small.

	A	B	C	D	E	F	G	H
1	Feature	Customer	Platform	Arista Contact	Arista RFE#	Comments	Status	In RFE Tracker
41	Broadcast, Multicast and	Telus		7500 Dave T	24026			yes
42	BSR	BNPP(FR)		7100 JP	14028			yes
43	Cisco like' CLI Ping behavior	Nomura-UK		7100 JP	14053	DONE		yes
44	Cli command to change	Fixnetix		7100 JP	9887			yes
45	Cli command to change	Virtu Financial,		7100 Lavanya	9887	Since EOS-		yes
46	Cli command to change	FCMME		7100 JP	7612			yes

(Feature: “Cisco like’ CLI Ping behavior”; Comments: “DONE”)

1	Feature	Customer	Platform	Arista Contact	Arista RFE#	Comments
33	Sh GateD conf in running config	Getco UK		7100 JP		
34	sh int trunk' command	DB		7100 JP		To mimic Cisco
35	Sh route count	Sevic		7100 Dave T		

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

(Feature: “sh int trunk” command”; Comments: “To mimic Cisco”)

	A	B	C	D	E	F	G	H
1	Feature	Customer	Platform	Arista Contact	Arista RFE#	Comments	Status	In RFE Tracker
154	BGP Advertisement Interval	Nomura	All	JP		http://www.cisco.com/en/US/docs/ios/12_3/iproute/command/reference/ip2_n1g.html#wp1036844		
155	BGP and OSPF MIBs	Chi-X	All	JP				
156	BGP Communities	Sawis	All	Dave T				

(Feature: “BGP Advertisement Interval”; Comments: link to Cisco website)

154. Arista's acts of copying with respect to the creative expressions in Cisco's programs including its CLI interface extend to not only programs such as all version of Arista's EOS operating system, but to printed and electronic documents distributed by Arista such as various versions of Arista User Manual for EOS and related documents used to train Arista's engineers, salesforce, distribution partners and customers.¹⁵¹ For example, Arista's User Manual

¹⁵¹ E.g., Arista Networks EOS User Manual Version 4.4.0 (CSI-CLI-00007473), Arista Networks EOS User Manual Version 4.0.1 (CSI-CLI-00007244), Arista Networks EOS User Manual Version 4.6.2 (CSI-CLI-00006858), Arista Networks EOS User Manual Version 4.10.0 (CSI-CLI-00007841), Arista Networks EOS User Manual Version 4.11.1 - Rev. 2 (CSI-CLI-00010517), Arista Networks EOS User Manual Version 4.11.2.1 (CSI-CLI-00008985), Arista Networks EOS User Manual Version 4.12.4 (CSI-CLI-00014141), Arista Networks EOS User Manual Version 4.13.7M (CSI-CLI-00011973), Arista Networks EOS User Manual Version 4.14.3F - Rev. 2 (CSI-CLI-00018146), Arista Networks EOS User Manual Version 4.14.5F -

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

for EOS contains unauthorized reproductions of Cisco’s copyrighted command expressions in its Command Reference section, as well in the detailed descriptions of such command expressions.¹⁵² Similarly, the same Arista manual also contains unauthorized reproductions of Cisco’s copyrighted screen displays.¹⁵³

B. Cisco’s CLI Documentation Compared to Arista’s CLI Documentation

155. I understand that Cisco contends that Arista has copied creative expressions in Cisco’s product documents that describe and relate to its CLI.¹⁵⁴ I agree with Cisco.

156. To start, I note that Arista’s CEO admitted at a technology conference after this lawsuit was filed that Arista copied copyrighted expressions in Cisco’s technical documents:

“The first claim is in the technical-documentation area, and they say that we have copied pieces of their documentation. We have done a thorough review over the weekend, and to the best of our ability we can see that—this is something that is completely unacceptable to me, that less than 1% has been copied. We are taking care of the individual and personnel who’s doing it. I own up to that. That’s a mistake. I apologize to Cisco for it. We’re going to fix it in a week.”¹⁵⁵

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Rev. 2 (CSI-CLI-00000084), Arista Networks EOS User Manual Version 4.14.6M (CSI-CLI-00004616), Arista Networks EOS User Manual Version 4.15.OF - Rev. 2.27 (CSI-CLI-00020575), Arista Networks EOS User Manual Version 4.15.0F (CSI-CLI-00002332), Arista Networks EOS User Manual Version 4.13.6F (CSI-CLI-00016001).

¹⁵² See, e.g., Exhibit Copying-1.

¹⁵³ See, e.g., Exhibit Copying-3.

¹⁵⁴ See Second Amended Complaint; see also Cisco’s responses to Interrogatory Nos. 2-4.

¹⁵⁵ CSI-CLI-00357842 at CSI-CLI-00357849 (emphasis added).

[REDACTED]

HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY – SOURCE CODE

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

158. I also have confirmed that there are many similarities between Arista's user manuals and Cisco's documents. The Arista user manuals that reflect these similarities include the following:

Date	Manual	Bates Begin	Bates End
4/8/2009	Arista Networks EOS User Manual Version 4.0.1	CSI-CLI-00007244	CSI-CLI-00007472
3/31/2010	Arista Networks EOS User Manual Version 4.4.0	CSI-CLI-00007473	CSI-CLI-00007840
3/28/2011	Arista Networks EOS User Manual Version 4.6.2	CSI-CLI-00006858	CSI-CLI-00007243
7/19/2012	Arista Networks EOS User Manual Version 4.10.0	CSI-CLI-00007841	CSI-CLI-00008984
1/22/2013	Arista Networks EOS User Manual Version 4.11.1 - Rev. 2	CSI-CLI-00010517	CSI-CLI-00011972
3/1/2013	Arista Networks EOS User Manual Version 4.11.2.1	CSI-CLI-00008985	CSI-CLI-00010516
9/16/2013	Arista Networks EOS User Manual Version 4.12.4	CSI-CLI-00014141	CSI-CLI-00016000
4/14/2014	Arista Networks EOS User Manual Version 4.13.6F	CSI-CLI-00016001	CSI-CLI-00018140
6/17/2014	Arista Networks EOS User Manual Version 4.13.7M	CSI-CLI-00011973	CSI-CLI-00014140
10/2/2014	Arista Networks EOS User Manual Version 4.14.3F - Rev. 2	CSI-CLI-00018146	CSI-CLI-00020337
12/22/2014	Arista Networks EOS User Manual Version 4.14.5F - Rev. 2	CSI-CLI-00000084	CSI-CLI-00002331
1/19/2015	Arista Networks EOS User Manual Version 4.14.6M	CSI-CLI-00004616	CSI-CLI-00006857
4/2015	Arista Networks EOS User Manual Version 4.15.OF - Rev. 2.27	CSI-CLI-00020575	CSI-CLI-00022852
4/18/2015	Arista Networks EOS User Manual Version 4.15.OF	CSI-CLI-00002332	CSI-CLI-00004615

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

(CSI-CLI-00016001, Arista User Manual v. 4.13.6F (4/14/2014), at 624)

166. Another example of strikingly similar structure arrangements—coupled with nearly verbatim word matching—exists in the description of security levels, Arista and Cisco list the same number/name for various severity levels with identical descriptions of each level:

<i>severity-level</i>	<p>(Optional) The number or name of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows (enter the number or the keyword):</p> <p>[0 emergencies] —System is unusable</p> <p>[1 alerts]—Immediate action needed</p> <p>[2 critical]—Critical conditions</p> <p>[3 errors]—Error conditions</p> <p>[4 warnings]—Warning conditions</p> <p>[5 notifications]—Normal but significant conditions</p> <p>[6 informational]—Informational messages</p> <p>[7 debugging]—Debugging messages</p>
-----------------------	--

(CSI-CLI-00291602, Cisco IOS Cisco Networking Services Command Reference (2013), at 91)

- **CONDITION** Specifies condition level. Options include:
 - <no parameter> Specifies default condition level.
 - **severity** <condition-level> Name of the severity level at which messages should be logged.

Valid *condition-level* options include:

- * 0 or **emergencies** System is unusable
- * 1 or **alerts** Immediate action needed
- * 2 or **critical** Critical conditions
- * 3 or **errors** Error conditions
- * 4 or **warnings** Warning conditions
- * 5 or **notifications** Normal but significant conditions
- * 6 or **informational** Informational messages
- * 7 or **debugging** Debugging messages

(CSI-CLI-00018146, Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 155)

167. I have attached Exhibit Copying-1 that sets forth additional instances of similarities found between Arista’s user manuals and Cisco’s copyrighted documentation. As

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

shown above and in Exhibit Copying-1, Arista’s manuals track Cisco’s copyrighted documents word-for-word in many places and/or they include nearly identical sentences and structural elements, such as tables and lists. As discussed below, Arista’s manuals also copy examples of Cisco’s screen outputs, and Arista also copied those outputs into EOS.

C. Cisco’s CLI Command Expressions Compared to Arista’s CLI Command Expressions

168. I understand that Cisco has asserted that Arista copied over 500 specific multi-word command expressions that are elements of the Cisco IOS copyrighted works.

169. Arista does not dispute that its products and documentation such as product manuals use these multi-word command expressions.¹⁵⁸ For example, Arista admitted such use in its answer to Cisco’s original complaint:¹⁵⁹

23 || 53. Arista admits that it uses the IOS command expressions included in Exhibit 1 to
24 || Cisco’s Complaint. Arista denies any remaining allegations of paragraph 53.

170. In its response to Interrogatory No. 9, for over 500 multi-word command expressions Arista provided the name of an Arista employee with knowledge of the command creation, development, and/or implementation as well as the approximate date of creation, development, and/or implementation. For example:

¹⁵⁸ See Arista’s responses to Cisco’s Interrogatory Nos. 9 (listing 516 commands) and 26 (listing 510 commands).

¹⁵⁹ Arista’s Answer to the Complaint (Dkt. 36) at ¶ 53.

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

173. To further confirm Arista’s use of the copied multi-word command expressions, I inputted commands into working versions of Arista’s switch running EOS made available by Arista in this litigation at its lawyers’ office. I also tested and inspected an Arista DCS-7048T-4S device running EOS 4.4.0 into which I also inputted multi-word command expressions.

174. When I input the commands, the Arista switch running EOS provided an output or response (not an error message) with the same look and feel as if I had inputted the commands into a Cisco device, which tells me that the multi-word command expressions are used in Arista’s EOS in precisely the same way as they are in Cisco’s IOS, and that a user would have a hard time knowing they were using an Arista switch instead of a Cisco switch. A log confirming my testing is provided as Exhibit Copying-7. The log confirms that EOS understands and knows how to respond to each of the commands, and that they are an integral part of EOS, including the CLI program with which the user interacts. I reserve the right to—and expect that as part of my trial testimony I will—demonstrate additional testing at trial, whether that be live or via video.

175. I do note that some of the multi-word command expressions Arista copied could not be run on the Arista switch in the limited environment provided by Arista. For certain commands to provide outputs, a live network environment is required to be set up and configured. During my inspections, however, the switches that Arista provided were not connected to a network or configured by Arista to simulate a live networking environment. Accordingly, my testing of commands that require a configured network was limited by the set up provided by Arista. Those limitations do not, however, impact my opinions, as I was able to

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

193. Because the evidence of Arista's use of Cisco's command hierarchies is voluminous, I have summarized the similarities in Exhibit Copying-5, which is incorporated here by reference.

F. Cisco's CLI Command Responses Compared to Arista's CLI Command Responses

194. As explained above, another aspect of Cisco's CLI is the textual, screen output generated by the CLI as feedback when the user inputs a particular command. Cisco contends that in many instances, Arista provides output displays in EOS that are similar if not identical to the displays in Cisco's CLI. I agree that there are very close similarities between the screen outputs in Cisco's CLI and Arista's CLI. In some instance, in fact, it is almost impossible for a user to tell if they are using a Cisco device or an Arista device—the similarities are that close.

[REDACTED]
 [REDACTED]
 [REDACTED]
 [REDACTED]

Response	Percentage
Yes, the U.S. should take action to address climate change	95%
No, the U.S. should not take action to address climate change	5%

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

```
[switch]>help
Help may be requested at any point in a command by entering
a question mark '?'. If nothing matches, the help list will
be empty and you must backup until entering a '?' shows the
available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show pr?').
```

(Cisco's Help Screen¹⁷⁰)

```
localhost#help
Help may be requested at any point in a command by entering
a question mark '?'. If nothing matches, the help list will
be empty and you must backup until entering a '?' shows the
available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
command argument (e.g. 'show ?') and describes each possible
argument.
2. Partial help is provided when an abbreviated argument is entered
and you want to know what arguments match the input
(e.g. 'show pr?'.)

localhost#
```

(Arista's Identical Help Screen in EOS 4.4.0¹⁷¹)

¹⁷⁰ See Exhibit Copying-7; see also CSI-CLI-00540145 at CSI-CLI-00540184.

¹⁷¹ See Exhibit Copying-7; e.g., ARISTANDCA 10485839 at ARISTANDCA 10485848; see also ARISTANDCA 10485836.

172 [REDACTED]

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

```

Arista 7xxx Arista:7xxx#show interfaces ethernet 1
Ethernet1 is up, line protocol is up (connected)
Hardware is Ethernet, address is 001c.7301.6010 (bia 001c.7301.6010)
MTU 9212 bytes, BW 10000000 Kbit
Full-duplex, 10Gb/s, auto negotiation: off
Last clearing of "show interface" counters never
5 seconds input rate 529 bps (0.0% with framing), 1 packets/sec
5 seconds output rate 979 bps (0.0% with framing), 1 packets/sec
8081820385 packets input, 4169996466948 bytes
Received 33 broadcasts, 48694 multicast
0 runs, 0 giants
0 input errors, 0 CRC, 0 alignment, 0 symbol
2 PAUSE input
2014734150 packets output, 137018818081 bytes
Sent 34 broadcasts, 2014899362 multicast
1 output errors, 0 collisions
0 late collision, 0 deferred
0 PAUSE output

Cisco 4948 RuiZ06#show int gigabitEthernet 1/1
GigabitEthernet1/1 is down, line protocol is down (not connected)
Hardware is Gigabit Ethernet Port, address is 8843.e1a4.2540 (bia 8843.e1a4.2540)
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
reliability 255/255, bioload 1/255, mload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Auto duplex, Auto speed, link type is auto, media type is 10/100/1000 TX
Input flow control is off, output flow control is off
Auto MDIX on (operational: on)
ARP type: ARPA, ARP Timeout 04:00:00
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts (0 multicasts)
0 runs, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 input packets with dribble condition detected
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 babbles, 0 late collision, 0 deferred

```

(ARISTANDCA12244293)

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

```

Arista 7xxx
Arista.7xxx#show int status
Port      Name      Status      Vlan    Duplex Speed Type
Et1        connected in Po1      full    10G 10GBASE-SR
Arista.71xx#dir
Directory of flash:/
-rwx- 221049088      Jul 22 06:12 EOS-4.7.5-448447.swi
-rwx- 32            Jul 28 22:45 boot-config
-rwx- 14            Jun 20 09:41 boot-extensions
-rwx- 4096          Aug 10 11:56 persist
-rwx- 7647          Aug 10 12:54 startup-config

Cisco 4948
Cisco.4948#dir
Directory of bootflash:/
 6 -rw- 24842288 Aug 13 2010 07:43:54 07:00 cat4500e-ent-services-mz.122-54.SG.bin
13 -rw- 26825925 Jul 18 2011 12:07:36 07:00 cat4500e-ent-servicesk9-mz.150-2.SG.bin

128282624 bytes total (68232320 bytes free)

```

(ARISTANDCA12244294)

```

Arista 7xxx
Arista.7xxx(config)#router ospf 1
Arista.7xxx(config-router-ospf)#router-id 1.1.1.1
Arista.7xxx(config-router-ospf)#network 10.10.10.0/24 area 0.0.0.0

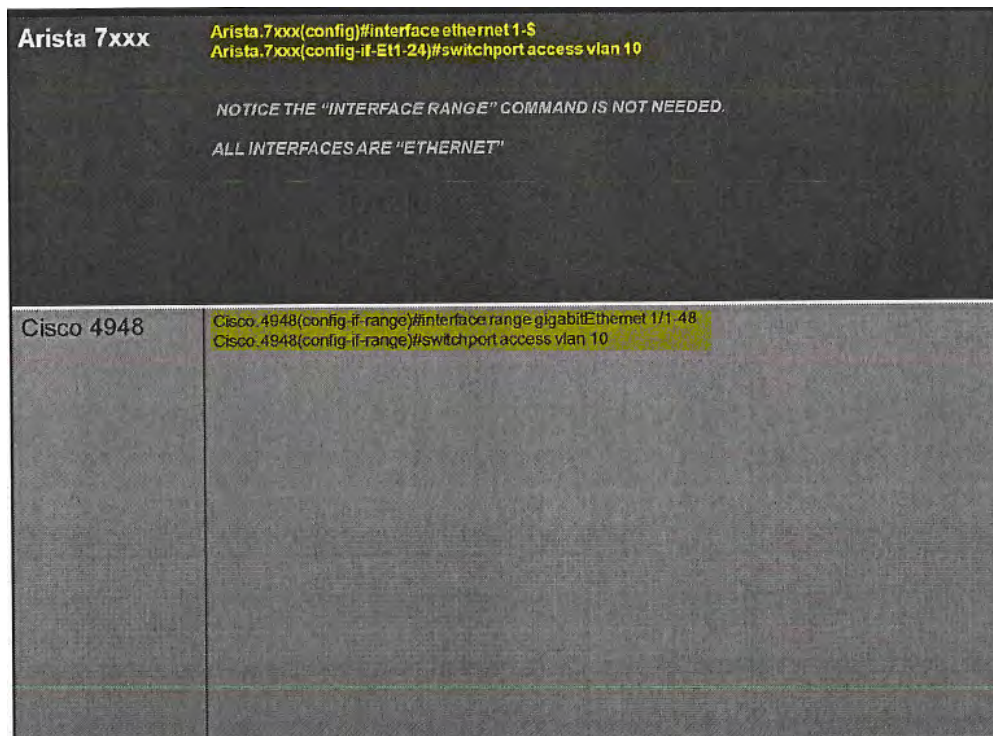
NOTICE THE USE CIDR MASK

Cisco 4948
Cisco.4948(config)#router ospf 1
Cisco.4948(config-router)#network 10.10.10.0/255.255.255.0 area 0.0.0.0

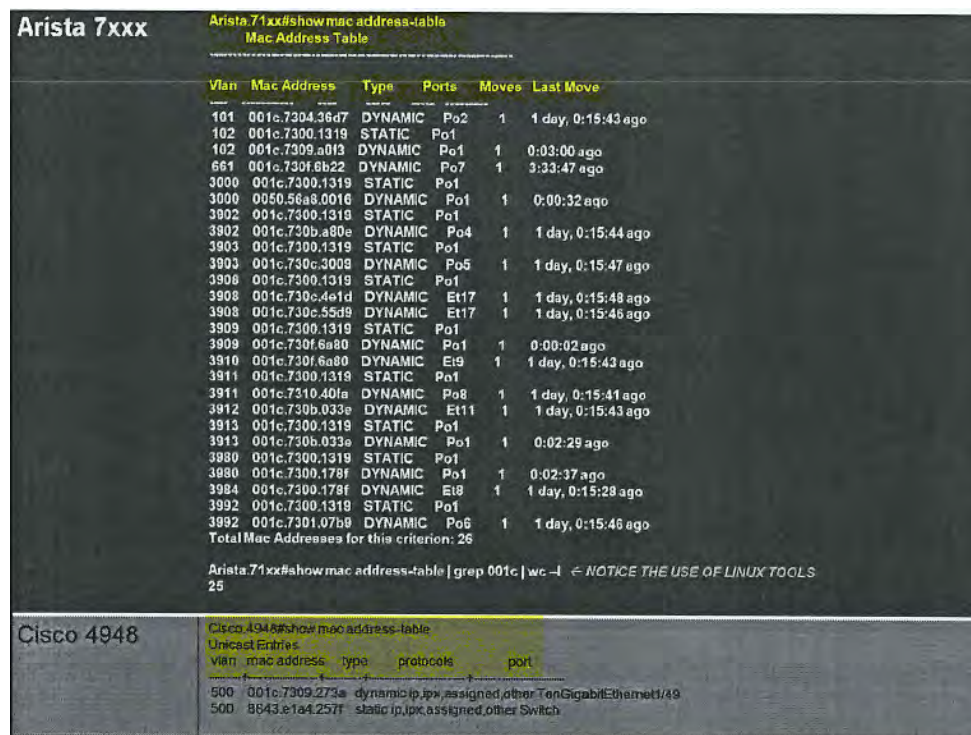
```

(ARISTANDCA12244295)

HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY – SOURCE CODE



(ARISTANDCA12244296)



(ARISTANDCA12244297)

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

be used in the same way as Cisco’s. Indeed, when sitting in front of an Arista switch running EOS, it is very difficult to know whether it is a Cisco switch running IOS or and Arista switch running EOS—they are similar.

224. As I discussed above in my description of Arista’s EOS programs, there are various unusual similarities between Cisco’s programs and Arista’s programs that suggest that, in fact, Arista developed EOS with knowledge of Cisco’s program. My descriptions of those similarities above are incorporated here by reference and support my belief that despite being written in different languages Arista’s EOS is similar to Cisco’s IOS in significant ways (*e.g.*, the parsing structure, use of specific tokens, etc.).

225. There also is evidence of direct copying by Arista of Cisco’s copyrighted works into Arista’s EOS programs. I understand that Cisco provided Exhibits G and H in response to Interrogatory No. 2. Those exhibits show hundreds of command help descriptions that appear in similar or identical form in both Cisco’s IOS and IOS-XR programs well as in Arista’s EOS programs. Here are just a few examples taken from Exhibit G:

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

Cisco HelpDesc	Same or Similar Arista HelpDesc	Arista File/Line
32-bit tag value	32-bit tag value	CliPlugin/RoutingOspfCli.py:2566
48-bit hardware address of ARP entry	48-bit hardware address of ARP entry	CliPlugin/IraIpCli.py:815
A regular-expression to match hostnames	A regular-expression to match	
AAA group definitions	AAA group definitions	AaaCliLib.py:207
ARP type ARPA	ARP type ARPA	CliPlugin/IraIpCli.py:817
ASBR summary link states	ASBR summary link states	CliPlugin/RoutingOspfCli.py:3094
Summary Access List	Access list summary	CliPlugin/AclCli.py:1156
Distance metric for this route	Administrative distance for this route	CliPlugin/PimCli.py:907
Administratively shut down this neighbor	Administratively shut \ down this neighbor	CliPlugin/RoutingBgpCli.py:2145
Administratively shut down this neighbor	Administratively shut \down this neighbor	CliPlugin/RoutingBgpCli.py:2145
Advertising Router (as an IP address)	Advertising Router (as an IP address)	
Advertising Router link states	Advertising Router link states	CliPlugin/RoutingOspf3Cli.py:1569
Always advertise default route	Always advertise default route	
An ordered list as a regular-expression	An ordered list as a regular-expression	CliPlugin/RouteMapCli.py:1760
Assign policy-map to the input of an interface	Assign policy-map to the input of an interface	CliPlugin/PbrCli.py:99
Assign policy-map to the output of an interface	Assign policy-map to the input of an interface	CliPlugin/PbrCli.py:99
Assign policy-map to the input of an interface	Assign policy-map to the output of an interface	CliPlugin/PbrCli.py:102
Assign policy-map to the output of an interface	Assign policy-map to the output of an interface	CliPlugin/PbrCli.py:102
authentication parameters for the user	Authentication parameters for the user	CliPlugin/SnmpCli.py:1582
encryption parameters for the user	Authentication parameters for the user	CliPlugin/SnmpCli.py:1582

(Exhibit G at 1)

Arista EOS 4.13.5: 'Specifies that an UNENCRYPTED key will follow' ->

Source Code/AaaCliLib.py:535

Cisco IOS-XR 514: 'Specifies that an UNENCRYPTED key will follow' ->

./aaa/protocols/radius/iox/radius_coa/src/cfg_dynamic_author_sub.cmd:77

./aaa/protocols/radius/iox/radius_coa/src/cfg_dynamic_author_sub.cmd:82

./aaa/protocols/radius/iox/radius_coa/src/cfg_dynamic_author_sub.cmd:141

(Exhibit H at 3)

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

```

Arista EOS 4.13.5: 'Exit from configure mode' ->
    Source Code/BasicCli.py:1058

Cisco IOS-XR 514: 'Exit from configure mode' ->
    ./parser/src/preload_admin_mode.cmd:29
    ./parser/src/preload_admin_mode.cmd:34
    ./parser/src/preload_admin_mode.cmd:40
    ./parser/src/preload_admin_mode.cmd:45
    ./parser/src/preload_config_mode.cmd:35
    ./parser/src/preload_config_mode.cmd:40
    ./parser/src/preload_config_mode.cmd:46
    ./parser/src/preload_config_mode.cmd:51

```

(Exhibit H at 5)

```

Arista EOS 4.13.5: 'Copy from current system configuration' ->
    Source Code/CliPlugin/FileCli.py:54

Cisco IOS-XR 514: 'Copy from current system configuration' ->
    ./shellutil/src/copy_admin.cmd:23
    ./shellutil/src/copy_admin.cmd:38

```

(Exhibit H at 18)

226. I have reviewed Exhibits G and H, and I have independently confirmed their content. Based on my review of these help descriptions, it is my opinion that the help descriptions are similar and in many instances word-for-word identical. In other words, there is evidence that Arista copied over 500 multi-word help descriptions from Cisco into its programs, and in doing so copied portions of Cisco’s programs.

227. I also performed testing to confirm these findings, and found evidence of copying as well. For example, the following screen shots show similarities between the help descriptions output with “show ?”:

HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY – SOURCE CODE

```

localhost>show ?
arp                ARP table
boot-extensions    Contents of boot extensions configuration
clock              Display the system clock
diagnostic          Show diagnostic tests
dot1q-tunnel        Show all enabled dot1q-tunnel ports
environment         Show environment status
errdisable          Show errdisable information
error              Show detailed information about an earlier error
extensions          EOS extensions present on this device
flowcontrol         Show interface flowcontrol information
history            Display the session command history
installed-extensions Installed EOS extensions
interfaces          Interface status and configuration
inventory           Display hardware inventory with serial numbers
ip                 IP information
lacp                Link Aggregation Control Protocol (LACP) status
lldp               Show Link Layer Discovery Protocol (LLDP) status
logging             Show the contents of logging buffers
mac-address-table   MAC forwarding table
mlag                MLAG status
monitor            Mirroring information
ntp                Network Time Protocol
port-channel        port-channel status
privilege           Display the current privilege level
processes           Show cpu and memory usage of running processes
radius              RADIUS server attributes
reload             Display system reload status
sflow              sFlow configuration
snmp                SNMP statistics
spanning-tree       Spanning tree topology
tacacs             TACACS+ server attributes
uptime             Show how long the system has been running
version            Show switch version information
vlan               Show VLAN status

```

(Arista)

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

```

Switch>show ?
aaa                Show AAA values
adjacency          Adjacent nodes
arp                ARP table
auto              Show Automation Template
cca               CCA information
class-map         Show QoS Class Map
clock             Display the system clock
cns               CNS agents
controllers        Interface controller status
crypto            Encryption module
dampening         Display dampening information
diagnostic        Show command for diagnostic
dot1q-tunnel      Display dot1q tunnel ports
dot1x             Dot1x information
eigrp             EIGRP show commands
env               Environmental facilities
epm               EPM information
errdisable        Error disable
etherchannel       EtherChannel information
exception         exception informations
flash:            display information about flash: file system
flowcontrol       show flow control information
format            Show format information
history           Display the session command history
hosts             IP domain-name, lookup style, nameservers, and host table
idprom            show IDPROMS for interfaces
if-mgr            if-mgr information
inventory         Show the physical inventory
ip                IP information
ipc              Interprocess communications commands
ipv6              IPv6 information
kerberos          Show Kerberos Values
kron              Kron Subsystem
l2                Layer 2
l2protocol-tunnel Display L2PT status and configurations
lacp              Port channel information
link              Show Link
lldp              LLDP information
location          Display the system location
login             Display Secure Login Configurations and State
mab               MAB information
mac               MAC configuration
macro             Show command macros
memory            Memory statistics
mls               mls global commands
monitor           Monitoring different system events
network-policy    Network Policy profile information
odm-format        Show the schema used for ODM input file
pagp              Port channel information
platform          platform specific show commands
pm               Show Port Manager commands
policy-map        Show QoS Policy Map
power             Switch Power
queue             Show queue contents
queueing          Show queueing configuration
radius            Shows radius information
resource          Resource group statistics
rmon              rmon statistics
sasl              show SASL information
sessions          Information about Telnet connections
shell             Display shell information
snmp              snmp statistics
ssh              Status of SSH server connections
ssl              Show SSL command
storm-control     Show storm control configuration
table-map         Show Table Map
tacacs            Shows tacacs+ server statistics
template          Template information
terminal          Display terminal configuration parameters
time-range        Time range
udld              UDLD information
users             Display information about terminal lines
version           System hardware and software status
vlan              VTP VLAN status

```

(Cisco)

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

228. The follow screen shots show similarities between the help descriptions output with “show interface ?” :

```
localhost>show interface ?  
Ethernet      Ethernet interface  
Loopback      Loopback interface  
Management    Management interface  
Port-Channel  Port-Channel Interface  
Vlan          Vlan interface  
capabilities  Show interface capabilities information  
counters      Interface counters  
description   Show interface description  
flowcontrol   Show interface flowcontrol information  
negotiation   Show interface Auto-Negotiation status  
phy           Display low-level PHY status  
status        Show interface line status  
switchport   Show interface switchport information  
transceiver   Show interface transceiver  
vlans         Show interface VLAN information  
|            Output modifiers  
<cr>
```

(Arista)

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

```

Switch>show interface ?
Async Async interface
Auto-Template Auto-Template interface
BVI Bridge-Group Virtual Interface
CTunnel CTunnel interface
Dialer Dialer interface
FastEthernet FastEthernet IEEE 802.3
Filter Filter interface
Filtergroup Filter Group interface
GigabitEthernet GigabitEthernet IEEE 802.3z
GroupVl Group Virtual interface
Loopback Loopback interface
Null Null interface
Port-channel Ethernet Channel of interfaces
Portgroup Portgroup interface
Pos-channel POS Channel of interfaces
Tunnel Tunnel interface
Vif PGM Multicast Host interface
Virtual-Template Virtual Template interface
Virtual-TokenRing Virtual TokenRing
Vlan Catalyst Vlans
accounting Show interface accounting
capabilities Show interface capabilities information
counters Show interface counters
crb Show interface routing/bridging info
dampening Show interface dampening info
debounce Show interface debounce time info
description Show interface description
etherchannel Show interface etherchannel information
fair-queue Show interface Weighted Fair Queueing (WFQ) info
fcpa Fiber Channel
flowcontrol Show interface flowcontrol information
irb Show interface routing/bridging info
mac-accounting Show interface MAC accounting info
mpls-exp Show interface MPLS experimental accounting info
mtu Show interface mtu
precedence Show interface precedence accounting info
private-vlan Show interface private vlan information
pruning Show interface trunk VTP pruning information
random-detect Show interface Weighted Random Early Detection (WRED)
info
rate-limit Show interface rate-limit info
stats Show interface packets & octets, in & out, by
switching path
status Show interface line status
summary Show interface summary
switchport Show interface switchport information
transceiver Show interface transceiver
trunk Show interface trunk information
| output modifiers

```

(Cisco)

229. The follow screen shots show similarities between the help descriptions output with “show ip ospf ?”:

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

```

Arista
-----
localhost(s1)#show ip ospf ?
border-routers      Border routers
database            Database summary
interface           Interface information
lsa-log             LSA throttling Log
neighbor            Neighbor information
request-list        Request list
retransmission-list Re-transmission list
spf-log             Spf Log
vrf                 VRF name
<1-65535>           Process ID
>                  Redirect output to URL
>>                 Append redirected output to URL
|                  Output modifiers
<cr>

```

(Arista)

```

Switch>show ip ospf ?
<1-65535>           Process ID number
border-routers      Border and Boundary Router Information
database            Database summary
interface           Interface information
max-metric           Max-metric origination information
mpls                MPLS related information
neighbor            Neighbor list
sham-links           Sham link information
statistics           Various OSPF Statistics
summary-address     Summary-address redistribution Information
timers              OSPF timers information
traffic             Traffic related statistics
virtual-links       Virtual link information
|                  Output modifiers
<cr>

```

(Cisco)

230. Because the evidence of Arista’s reproduction of Cisco’s help descriptions into EOS is voluminous, I have summarized the similarities in Exhibit Copying-6, which is incorporated here by reference.

VII. THERE IS NO INDUSTRY STANDARD FOR CISCO’S COPYRIGHTED WORKS

231. I understand that Arista contends that it is permitted to use Cisco’s IOS CLI because Cisco’s IOS is an “industry standard.” As explained below, I disagree with Arista and

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

- [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

- [REDACTED]
[REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED] [REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

- [REDACTED] [REDACTED] [REDACTED]

[REDACTED]

- [REDACTED] [REDACTED] [REDACTED]

[REDACTED]

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

Government	Percentage
Current government	55%
Previous government	45%

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

243. I also have found evidence that Arista implements at least 11 additional multi-word command expressions that are not used by IOS but are from one of Cisco’s other operating systems (IOS-XR, IOS-XE, NX-OS). This further proves that Arista’s copying of Cisco goes beyond even what it contends to be “industry standard” elements:

Other Cisco OS Except IOS

interface ethernet
 ip dhcp smart-relay global
 log-adjacency-changes (IS- IS)
 policy-map type qos
 show environment power
 show isis interface
 show lacp counters
 show mac address-table count
 show port-security interface
 show radius
 show spanning-tree mst interface

244. Arista’s interrogatory response to Cisco’s Interrogatory No. 10 further confirms that there is a lot of diversity in command and mode choice and use in the industry.¹⁸⁶ Indeed, what Arista’s own analysis shows is that some industry participations—like IBM—do not use any of the so-called “industry standard” multi-word commands that Arista copied from Cisco and that many participates use their own modes/prompts as well:

¹⁸⁶ I have assumed for purposes of this report only that Arista’s response to Interrogatory No. 10 is accurate.

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

245. Further, even though the term “industry standard” may be used by some in the industry when marketing their products for different context, there is, in fact, no industry standard command line interface computer program let alone an industry standard for the Cisco CLI.¹⁸⁷ Based on my review of the evidence and knowledge of the industry, I have seen no evidence that Cisco’s CLI is part of an industry standard. Industry standard protocols typically specify how data is sent from device-to-device—they do not specify implementation choices by vendors, including user interfaces, command selection, command hierarchical relationships, documentation, or screen outputs, which are influenced by subjective vendor preferences. Thus, it does not surprise me that there is no industry standard for Cisco’s copyrighted works. Not only is there diversity in the multi-word command expressions, there is diversity in the help screens, outputs, and other display screens.

■ [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

¹⁸⁷ See, e.g., Cisco’s responses to Arista’s Interrogatory No. 9.

■ [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

247. Additionally, I have seen no evidence to suggest that Cisco ever proposed its CLI to a standards-setting body¹⁹² or that Cisco requires others in the industry to use its CLI. According to Cisco, when the term “industry standard” is used in Cisco’s marketing materials, it refers to “the popularity and quality of Cisco’s CLI in Cisco’s industry leading products.”¹⁹³ It does not refer to an industry standard adopted by an industry standard setting organization, such as the IEEE and IETF.¹⁹⁴ I have independently confirmed this to be true—neither the IEEE nor the IETF has adopted Cisco’s CLI as a standard. And I have seen no evidence from Arista that any other standard setting body adopted Cisco’s CLI as a standard. I also have not seen any

Testimony of Foss; Deposition Testimony of Hull; Deposition Testimony of Pech; Deposition Testimony of Redlefsen; Deposition Testimony of Sollender; *see also* the deposition testimony identified in response to Arista’s Interrogatory No. 21, which is incorporated here by reference.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

¹⁹² *See, e.g.*, Deposition Testimony of Lang, Bechtolsheim, Berly, Ullal; *see also* the deposition testimony identified in response to Arista’s Interrogatory No. 21, which is incorporated here by reference.

¹⁹³ *See, e.g.*, Cisco’s responses to Arista’s Interrogatory No. 9.

¹⁹⁴ *See, e.g.*, Cisco’s responses to Arista’s Interrogatory No. 9.

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

evidence to suggest that Cisco has given any competitors permission to copy or to use substantial portions of its CLI.¹⁹⁵

248. Furthermore, as it relates to the screen displays, command descriptions, and documentation that Arista has copied, I have not seen any allegation by Arista that those particular elements are in any way “industry standard.” In fact, Arista’s definition of the term “industry standard” mentions none of those elements:

“The term ‘industry standard CLI’ refers to CLI commands, and the attendant command modes, prompts, and hierarchies, that are widely recognized and supported by other networking vendor CLIs regardless of whether they are used by Cisco across all of its various operating systems. The ‘industry standard CLI’ also means the CLI commands and attendant CLI functionality that most customers—and in particular, most end-users who interact with the networking equipment—are most familiar with, have used for years, and have invested time and resources to learn.”¹⁹⁶

249. Even assuming for the sake of argument that the elements Arista lists are part of some “industry standard”—commands, modes, prompts, hierarches, functions—it is not disputed by Arista that the many other elements of Cisco’s copyrighted works that Arista copied do not even fall within Arista’s definition of “industry standard.” Accordingly, Arista has not made any “industry standard” argument for its copying of at least Cisco’s screen displays, help descriptions, command descriptions, and documentation.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

¹⁹⁵ See, e.g., Deposition Testimony of Jiandani, Roy, and Lang (7/31/15).

¹⁹⁶ Arista’s response to Cisco’s Interrogatory No. 24.

¹⁹⁷ A [REDACTED]

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

■ ■ [REDACTED]
 ■ [REDACTED]
 ■ [REDACTED]
 ■ [REDACTED]
 ■ [REDACTED]
 ■ [REDACTED]
 ■ [REDACTED]
 ■ [REDACTED]
 ■ [REDACTED]
 ■ [REDACTED]
 ■ [REDACTED]

253. In sum, it is my opinion that the evidence does not show that there is any industry standard CLI let alone that Cisco’s IOS CLI in an industry standard CLI.

VIII. CONTRIBUTORY INFRINGEMENT & VICARIOUS LIABILITY

254. I understand that Cisco contends that Arista also has contributed to the infringement of others, including its distributors and customers. It is my understanding that contributory infringement requires third party copying, knowledge by the defendant, and material contribution or inducement.

255. Arista’s EOS and its related-documents copy original expressions from Cisco’s IOS copyright works, as discussed in detail above.

256. I conclude that Arista strongly encourages its customers to use Arista products incorporating EOS—as well as Arista user manuals and guides that Arista admits it supplies²⁰³—for reproduction and distribution on their devices. Arista provides products, programs, and technical support so that its distributors and/or customers may use Arista’s EOS and/or EOS+ operating systems and its command-line interface computer program, which infringe Cisco’s copyrights in the Cisco IOS Copyrighted Works. Arista has numerous publicly available webpages dedicated to encouraging and overseeing the use of its products that incorporate

²⁰³ Arista’s answer to Cisco’s Second Amended Complaint at ¶ 55.

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

Cisco’s copyright works through product documentation, training,²⁰⁴ forums, or support.²⁰⁵ The only reason for selling products to customers and supplying customers with supporting documents is to encourage Arista’s customers to use its products that incorporate Cisco’s copyright works. In fact, Arista has publicly admitted that at least 80% of its customers consider this infringing functionality to be an important factor in their decisions to purchase Arista’s products.²⁰⁶

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

²⁰⁴ Deposition of Sadana (Rough) Tr. at 111:5-21, 112:20-113:3, 114:17-116:1, 116:19-117:4, 117:16-19, 118:15-120:1, 120:18-121:19, 123:16-124:8, 125:6-12, (May 26, 2016); Deposition of Sadana (Rough) Tr. at 101:6-9, 104:3-17 (May 27, 2016).

²⁰⁵ See, e.g., <https://www.arista.com/en/support/product-documentation>; <https://www.arista.com/en/support/hands-on-training>; <http://solutions.arista.com/training>; <http://solutions.arista.com/workshop-training> (“Understanding the capabilities of the EOS CLI and Linux Bash access” including various modules on the EOS CLI); <https://www.arista.com/en/support/customer-support>; <https://eos.arista.com/>.

²⁰⁶ CSI-CLI-00540078 at CSI-CLI-00540079.

Category	Percentage
U.S. should take action	85%
U.S. should not take action	15%

[REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

²⁰⁷ E.g., ARISTANDCA11996066, ARISTANDCA104437, ARISTANDCA1206372, ANI-ITC-944_945-3473603, ARISTANDCA1199299, ANI-ITC-944_945-3927203, ARISTANDCA10499890, ARISTANDCA_SW_105998, CSI-ANI-00381280, ARISTANDCA11411864, ARISTANDCA10499890, ANI-ITC-944_945-3452525, ARISTANDCA1194925, CSI-CLI-00540078, Packet Pushers Clip (Audio File) (Duda Exh. 274), Sadana Deposition, Exhibit 382, at 78, Posting of Kenneth Duda to Arista EOS Central, “Linux as a Switch Operating System: Five Lessons Learned” (Nov. 5, 2013), *available at* <https://eos.arista.com/linux-as-a-switch-operating-system-five-lessons-learned/>.

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

its customers and distributors: Arista is a publicly traded company and derives value from the sale of products that contain computer programs and/or other works that infringe Cisco’s copyrights. Furthermore, Arista has the right and ability to supervise at least the use, reproduction, distribution, and/or public display of computer programs and/or other works that infringe Cisco’s copyrights by at least Arista’s distributors and/or customers.

IX. CISCO’S COPYRIGHTED WORKS WERE NOT COPIED FROM STANFORD

259. I understand that Arista generally alleges that Cisco may not own its copyrighted works because they “are not Cisco’s intellectual property, are derived from prior works over which Cisco has no ownership rights with respect to copyright assertions, and/or may not be asserted by Cisco in a copyright infringement action.”²⁰⁸ Specifically, I understand that Arista has made vague allegations relating to work Mr. Loughheed did at Stanford, on “TOPS-20,” and worked related to SUMEX.²⁰⁹

260. Although Arista has not formulated a clear theory or argument setting forth with any specificity which of the copyrighted works it contends came from Stanford or TOPS-20, I have nevertheless reviewed Mr. Loughheed’s deposition testimony, spoken with Mr. Loughheed, and reviewed the source code relating to Arista’s Stanford allegations.²¹⁰ In sum, I have not seen any evidence that the multi-word command expressions (along with their specific associated modes and prompts) asserted in this case—or any of the other elements at issue in this case from the copyrighted works—originated from anywhere other than Cisco, nor have I seen any

²⁰⁸ Arista’s response to Interrogatory No. 10.

²⁰⁹ *Id.*

²¹⁰ *See also, e.g.*, KL-00000564; KL-00000186; KL-00000381; KL-00000655, KL-00000251; KL-SC-00000033 to 52; KL-00000001.

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

evidence to suggest that Cisco copied them. In fact, Cisco has provided voluminous information detailing the provenance of the multi-word command expressions at issue in this case.²¹¹

261. Further, in my opinion, the source code Mr. Lougheed worked on while at Stanford is different than the source code he developed during that same time for Cisco. Mr. Lougheed confirmed this to me as well.²¹² The fact that certain single word commands or protocols—e.g., “show,” “clear,” “help,” “ip,” “no,” “arp,” “bgp”—existed before Cisco does not show (or prove) that any of Cisco’s copyrighted works were copied, nor does it suggest to me that the copyrighted works are unoriginal. If Arista puts forth a more coherent and clear theory or argument in its expert report that actually explains what its allegations are, I reserve the right to supplement this report and/or respond to such allegations.

X. CONCLUSION

262. For presentation of my testimony at trial I may create and use demonstratives, videos, and/or additional screenshots of the copyrighted works described in this report. In addition, I may demonstrate the use of one or more Arista and Cisco switches at trial in support of my testimony.

263. I reserve the right to supplement or amend my opinions in response to opinions expressed by Arista’s experts, or in light of any additional evidence, testimony, discovery or other information that may be provided to me after the date of this report. In addition, I reserve the right to consider and testify about issues that may be raised by Arista’s fact witnesses and

²¹¹ See Cisco’s responses to Arista’s Interrogatory Nos. 2, 16, 19.

²¹² Conversation with Kirk Lougheed (June 2, 2016); *see also* Lougheed Deposition Tr. 129:5-130:19, 166:24-169:16 (“I didn’t like his lack of hierarchy”; “I started building a hierarchy”) (Nov. 20, 2015); Lougheed Deposition Tr. 332:6-23, 339:18-340:9 (April 4, 2016).

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY – SOURCE CODE

experts at trial. I also reserve the right to modify or to supplement my opinions as a result of ongoing expert discovery or testimony at trial.

I certify under penalty of perjury that the foregoing is true and correct.



By: 
Dr. Kevin C. Almeroth
June 3, 2016

Exhibit Copying-1 – Evidence of Documentation Copying

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS XE 3.5</p> <p>Effective date of registration: 11/24/2014</p>	<p>Usage Guidelines For additional notification types, see the Related Commands table for this command.</p> <p>SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types. To specify whether the notifications should be sent as traps or informs, use the snmp-server host [traps informs] command.</p> <p>If you do not enter an snmp-server enable traps command, no notifications controlled by this command are sent. In order to configure the router to send these SNMP notifications, you must enter at least one snmp-server enable traps command. If you enter the command with no keywords, all notification types are enabled. If you enter the command with a keyword, only the notification type related to that keyword is enabled. In order to enable multiple types of notifications, you must issue a separate snmp-server enable traps command for each notification type and notification option.</p> <p>The snmp-server enable traps command is used in conjunction with the snmp-server host command. Use the snmp-server host command to specify which host or hosts receive SNMP notifications. In order to send notifications, you must configure at least one snmp-server host command.</p> <p>Cisco IOS Configuration Fundamentals and Network Management Command Reference (2004), at 1034; <i>see also</i> Cisco IOS Asynchronous Transfer Mode Command Reference (2011), at 535.</p>	<p>snmp-server enable traps</p> <p>The snmp-server enable traps command enables the transmission of Simple Network Management Protocol (SNMP) notifications as traps or inform requests. This command enables both traps and inform requests for the specified notification types. The snmp-server host command specifies the notification</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1990.</p> <p><i>See also</i> Arista User Manual v. 4.13.6F (4/14/2014), at 1918; Arista User Manual v. 4.12.3 (7/17/13), at 1680; Arista User Manual, v. 4.11.1 (1/11/13), at 1365; Arista User Manual v. 4.10.3 (10/22/12), at 1132; Arista User Manual v. 4.9.3.2 (5/3/12), at 888; Arista User Manual v. 4.8.2 (11/18/11), at 696; Arista User Manual v. 4.7.3 (7/18/11), at 552.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS XE 3.5</p> <p>Effective date of registration: 11/24/2014</p>	<pre>Router# show interfaces atm 0/0/0 ATM0/0/0 is up, line protocol is up Hardware is cyBus ATM Internet address is 10.1.1.1/24 MTU 4470 bytes, sub MTU 4470, BW 156250 Kbit, DLY 80 usec, rely 255/255, load 1/255 Encapsulation ATM, loopback not set, keepalive set (10 sec) Encapsulation(s): AAL5, PVC mode 256 TX buffers, 256 RX buffers, 2048 maximum active VCs, 1024 VCs per VP, 1 current VCCs VC idle disconnect time: 300 seconds Last input never, output 00:00:05, output hang never Last clearing of "show interface" counters never Queueing strategy: fifo Output queue 0/40, 0 drops; input queue 0/75, 0 drops 5 minute input rate 0 bits/sec, 1 packets/sec 5 minute output rate 0 bits/sec, 1 packets/sec 5 packets input, 560 bytes, 0 no buffer Received 0 broadcasts, 0 runts, 0 giants 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort 5 packets output, 560 bytes, 0 underruns 0 output errors, 0 collisions, 0 interface resets 0 output buffer failures, 0 output buffers swapped out</pre> <p>Cisco IOS Asynchronous Transfer Mode Command Reference (2011), at 476.</p>	<p>Examples</p> <ul style="list-style-type: none"> These commands display interface counters, clear the counters, then display the counters again. <pre>switch#show interfaces ethernet 1 Ethernet1 is up, line protocol is up (connected) Hardware is Ethernet, address is 001c.7302.2fff (bia 001c.7302.2fff) MTU 9212 bytes, BW 10000000 Kbit Full-duplex, 10Gb/s, auto negotiation: off Last clearing of "show interface" counters never 5 minutes input rate 101 bps (0.0% with framing), 0 packets/sec 5 minutes output rate 0 bps (0.0% with framing), 0 packets/sec 21997/5554000 packets input, 228028532832583 bytes Received 29769609741 broadcasts, 3072437605 multicast 113 runts, 1 giants 118 input errors, 117 CRC, 0 alignment, 18 symbol 27511409 PAUSE input 335031607678 packets output, 27845413138330 bytes Sent 14282316688 broadcasts, 54045824072 multicast 108 output errors, 0 collisions 0 late collision, 0 deferred 0 PAUSE output</pre> <p>Arista User Manual v. 4.13.6F (4/14/2014), at 637.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 514; Arista User Manual, v. 4.11.1 (1/11/13), at 413; Arista User Manual v. 4.10.3 (10/22/12), at 270; Arista User Manual v. 4.9.3.2 (5/3/12), at 252.</p>
<p>Cisco IOS XE 3.5</p> <p>Effective date of registration: 11/24/2014</p>	<p>show vrrp</p> <p>To display a brief or detailed status of one or all configured Virtual Router Redundancy Protocol (VRRP) groups on the router, use the show vrrp command in privileged EXEC mode.</p> <p>show vrrp [all brief]</p> <p>Cisco IOS IP Application Services Command Reference (2011), at 76.</p>	<p>19.2.3.2 Verify VRRP IPv6 Configurations</p> <p>Use the following commands to display the VRRP configurations and status.</p> <p>Show VRRP Group</p> <p>The show vrrp command displays the status of configured Virtual Router Redundancy Protocol (VRRP) groups on a specified interface.</p> <p>Arista User Manual v. 4.13.6F (4/14/2014), at 879.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 793; Arista User Manual v. 4.10.3 (10/22/12), at 548; Arista User Manual v. 4.9.3.2 (5/3/12), at 468.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 15.2</p> <p>Effective date of registration: 11/24/2014</p>	<p>Usage Guidelines Use the <code>ip multicast multipath</code> command to enable load splitting of IP multicast traffic across multiple equal-cost paths.</p> <p>If two or more equal-cost paths from a source are available, unicast traffic will be load split across those paths. However, by default, multicast traffic is not load split across multiple equal-cost paths. In general, multicast traffic flows down from the reverse path forwarding (RPF) neighbor. According to the Protocol Independent Multicast (PIM) specifications, this neighbor must have the highest IP address if more than one neighbor has the same metric.</p> <p>Configuring load splitting with the <code>ip multicast multipath</code> command causes the system to load split multicast traffic across multiple equal-cost paths based on source address using the S-hash algorithm. When the <code>ip multicast multipath</code> command is configured and multiple equal-cost paths exist, the path in which multicast traffic will travel is selected based on the source IP address. Multicast traffic from different sources will be load split across the different equal-cost paths. Load splitting will not occur across equal-cost paths for multicast traffic from the same source sent to different multicast groups.</p> <p>Cisco IOS IP Multicast Command Reference (2011), at 293.</p>	<p>23.3.2 Equal Cost Multipath Routing (ECMP) and Load Sharing</p> <p>Multiple routes that have identical destinations and administrative distances comprise an Equal Cost Multi-Path (ECMP) route. The switch attempts to spread traffic to all ECMP route paths equally.</p> <p>If two or more equal-cost paths from a source are available, unicast traffic is load split across those paths. By default, multicast traffic is not load split. Multicast traffic generally flows from the reverse path forwarding (RPF) neighbor and, according to Protocol Independent Multicast (PIM) specifications, the neighbor with the highest IP address has precedence when multiple neighbors have the same metric.</p> <p>Arista User Manual v. 4.13.6F (4/14/2014), at 1191.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1042; Arista User Manual, v. 4.11.1 (1/11/13), at 398; Arista User Manual v. 4.10.3 (10/22/12), at 320.</p>
<p>Cisco IOS 15.2</p> <p>Effective date of registration: 11/24/2014</p>	<p>Usage Guidelines Use the <code>ip multicast boundary</code> command to configure an administratively scoped boundary on an interface in order to filter source traffic coming into the interface and prevent mroute states from being created on the interface.</p> <p> Note An IP multicast boundary enables reuse of the same multicast group address in different administrative domains.</p> <p>Cisco IOS IP Multicast Command Reference (2011), at 264.</p>	<p>Multicast Boundary Configuration</p> <p>The multicast boundary specifies subnets where source traffic entering an interface is filtered to prevent the creation of mroute states on the interface. The interface is not included in the outgoing interface list (OIL). Multicast pim, igmp or data packets are not allowed to flow across the boundary from either direction. The boundary facilitates the use of a multicast group address in different administrative domains.</p> <p>The <code>ip multicast boundary</code> command configures the multicast boundary. The multicast boundary can be specified through multiple IPv4 subnets or one standard IPv4 ACL.</p> <p>Arista User Manual v. 4.13.6F (4/14/2014), at 1704.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1482; Arista User Manual, v. 4.11.1 (1/11/13), at 1184; Arista User Manual v. 4.10.3 (10/22/12), at 1018; Arista User Manual v. 4.9.3.2 (5/3/12), at 776.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 15.0</p> <p>Effective Date of Registration: 11/28/2014</p>	<p>Usage Guidelines Enabling PIM on an interface also enables Internet Group Management Protocol (IGMP) operation on that interface. An interface can be configured to be in dense mode, sparse mode, or sparse-dense mode. The mode describes how the Cisco IOS software populates its multicast routing table and how the software forwards multicast packets it receives from its directly connected LANs. Dense mode interfaces are always added to the table when the multicast routing table is populated. Sparse mode interfaces are added to the table only when periodic join messages are received from downstream routers, or there is a directly connected member on the interface.</p> <p>Cisco IOS IP Multicast Command Reference (2008), at IMC-233–34</p>	<p>33.3.1 Enabling IGMP</p> <p>Enabling PIM on an interface also enables IGMP on that interface. When the switch populates the multicast routing table, interfaces are added to the table only when periodic join messages are received from downstream routers, or when there is a directly connected member on the interface.</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1778.</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 1726; Arista User Manual v. 4.12.3 (7/17/13), at 1504; Arista User Manual, v. 4.11.1 (1/11/13), at 1204; Arista User Manual v. 4.10.3 (10/22/12), at 998; Arista User Manual v. 4.9.3.2 (5/3/12), at 756; Arista User Manual v. 4.8.2 at 578; Arista User Manual v. 4.7.3 (7/18/11), at 458; Arista User Manual v. 4.6.0 (12/22/2010), at 308</p>
<p>Cisco IOS 15.2</p> <p>Effective date of registration: 11/24/2014</p>	<p>Usage Guidelines SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types. PIM notifications are defined in the CISCO-PIM-MIB.mib and PIM-MIB.mib files, available from Cisco.com at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.</p> <p>Cisco IOS IP Multicast Command Reference (2011), at 742</p>	<p>SNMP Commands Chapter 37 SNMP</p> <p>snmp-server enable traps</p> <p>The snmp-server enable traps command enables the transmission of Simple Network Management Protocol (SNMP) notifications as traps or inform requests. This command enables both traps and inform requests for the specified notification types. The snmp-server host command specifies the notification type (traps or informs). Sending notifications requires at least one snmp-server host command.</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1990.</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 1918; Arista User Manual v. 4.12.3 (7/17/13), at 1680; Arista User Manual, v. 4.11.1 (1/11/13), at 1365; Arista User Manual v. 4.10.3 (10/22/12), at 1132; Arista User Manual v. 4.9.3.2 (5/3/12), at 888; Arista User Manual v. 4.8.2 at 696; Arista User Manual v. 4.7.3 (7/18/11), at 552.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 15.2</p> <p>Effective date of registration: 11/24/2014</p>	<p>Usage Guidelines The local proxy ARP feature allows the Multilayer Switching Feature Card (MSFC) to respond to ARP requests for IP addresses within a subnet where normally no routing is required. With the local proxy ARP feature enabled, the MSFC responds to an ARP request for IP addresses within the subnet and forwards all traffic between hosts in the subnet. Use this feature only on subnets where hosts are intentionally prevented from communicating directly to the Catalyst 6500 series switch on which they are connected.</p> <p>Before the local proxy ARP feature can be used, the IP proxy ARP feature must be enabled. The IP proxy ARP feature is enabled by default.</p> <p>Cisco IOS IP Addressing Services Command Reference (2011), at 394</p>	<p>ip local-proxy-arp</p> <p>The <code>ip local-proxy-arp</code> command enables local proxy ARP (Address Resolution Protocol) on the configuration mode interface. Local proxy ARP programs the switch to respond to ARP requests for IP addresses within a subnet where routing is not normally required. A typical local proxy arp application is supporting isolated private VLANs that communicate with each other by routing packets.</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1276.</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 1231; Arista User Manual v. 4.12.3 (7/17/13), at 1073; Arista User Manual, v. 4.11.1 (1/11/13), at 856; Arista User Manual v. 4.10.3 (10/22/12), at 707.</p>
<p>Cisco IOS 15.2</p> <p>Effective date of registration: 11/24/2014</p>	<p>Usage Guidelines IP uses a 32-bit mask that indicates which address bits belong to the network and subnetwork fields, and which bits belong to the host field. This is called a <i>netmask</i>. By default, <code>show</code> commands display an IP address and then its netmask in dotted decimal notation. For example, a subnet would be displayed as 10.108.11.0 255.255.255.0.</p> <p>Cisco IOS IP Addressing Services Command Reference (2011), at 452</p>	<ul style="list-style-type: none"> • SUBNET_SIZE this functions as a sanity check to ensure it is not a network or broadcast network. Options include: <ul style="list-style-type: none"> — netmask ipaddr The network mask that indicates which address bits belong to the network and subnetwork fields and which bits belong to the host field. Specify the netmask of the network to which the pool addresses belong (dotted decimal notation). <p>Arista User Manual v. 4.13.6F (4/14/2014), at 1233.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1075.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 12.4</p> <p>Effective date of registration: 8/12/2005</p>	<p>Route Target Extended Community Attribute</p> <p>The route target (RT) extended community attribute is configured with the rt keyword. This attribute is used to identify a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that are used for routing traffic that is received from corresponding sites.</p> <p>Site of Origin Extended Community Attribute</p> <p>The site of origin (SOO) extended community attribute is configured with the soo keyword. This attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a particular site must be assigned the same site of origin extended community attribute, regardless if a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents routing loops from occurring when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed.</p> <p>IP Extended Community-List Configuration Mode</p> <p>Named and numbered extended community lists can be configured in IP Extended community-list configuration mode. To enter IP Extended community-list configuration mode, enter the ip extcommunity-list command with either the expanded or standard keyword followed by the extended community list name. This configuration mode supports all of the functions that are available in global configuration mode. In addition, you can perform the following operations:</p> <p>Cisco IOS IP Routing Protocols Command Reference, Release 12.4 (2005), at IRP-118</p>	<p>ip extcommunity-list expanded</p> <p>The ip extcommunity-list expanded command creates an extended community list to configure Virtual Private Network (VPN) route filtering. Extended community attributes filter routes for virtual routing and forwarding instances (VRFs). The command uses regular expressions to name the communities specified by the list.</p> <ul style="list-style-type: none"> • Route Target (rt) attribute identifies a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that route traffic received from corresponding sites. • Site of Origin (soo) attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a specific site must be assigned the same site of origin attribute whether a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents the creation of routing loops when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed. <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1590.</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 1540; Arista User Manual v. 4.12.3 (7/17/13), at 1364; Arista User Manual, v. 4.11.1 (1/11/13), at 1110; Arista User Manual v. 4.10.3 (10/22/12), at 896; Arista User Manual v. 4.9.3.2 (5/3/12), at 689; Arista User Manual v. 4.8.2 at 519.</p>
<p>Cisco IOS 15.2</p> <p>Effective date of registration: 11/24/2014</p>	<p>Usage Guidelines</p> <p>Extended community attributes are used to configure, filter, and identify routes for virtual routing and forwarding instances (VRFs) and Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs).</p> <p>The match extcommunity command is used to configure match clauses that use extended community attributes in route maps. All of the standard rules of match and set clauses apply to the configuration of extended community attributes.</p> <p>Cisco IOS IP Routing: EIGRP Command Reference (2011), at 92</p>	<p>BGP extended communities configure, filter, and identify routes for virtual routing, forwarding instances (VRFs), and Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs).</p> <p>Extended community clauses provide route target and site of origin parameter options:</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1552.</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 1502; Arista User Manual v. 4.12.3 (7/17/13), at 1334; Arista User Manual, v. 4.11.1 (1/11/13), at 1083; Arista User Manual v. 4.10.3 (10/22/12), at 896; Arista User Manual v. 4.9.3.2 (5/3/12), at 668; Arista User Manual v. 4.8.2 (11/18/11) at 500.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 12.4</p> <p>Effective date of registration: 8/12/2005</p>	<p>Expanded Community Lists</p> <p>Expanded community lists are used to filter communities using a regular expression. Regular expressions are used to configure patterns to match community attributes. The order for matching using the * or + character is longest construct first. Nested constructs are matched from the outside in.</p> <p>Concatenated constructs are matched beginning at the left side. If a regular expression can match two different parts of an input string, it will match the earliest part first. For more information about configuring regular expressions, see the Regular Expressions appendix of the <i>Cisco IOS Terminal Services Configuration Guide</i>.</p> <p>Cisco IOS IP Routing Protocols Command Reference, Release 12.4 (2005), at IRP-113–14</p>	<p>Chapter 3 Command-Line Interface Processing Commands</p> <pre> ~rxy\$ ~rxy 23 21 rxy .rxy. rxy .rxy. </pre> <p>The order for matching using the * or + character is longest construct first. Nested constructs are matched from the outside in. Concatenated constructs are matched beginning at the left side. If a regular expression can match two different parts of an input string, it matches the earliest part first.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 107.</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 105; Arista User Manual v. 4.12.3 (7/17/13), at 95; Arista User Manual, v. 4.11.1 (1/11/13), at 65; Arista User Manual v. 4.10.3 (10/22/12), at 57; Arista User Manual v. 4.9.3.2 (5/3/12), at 53; Arista User Manual v. 4.8.2 (11/18/11), at 49.</p>
<p>Cisco IOS 12.4</p> <p>Effective date of registration: 8/12/2005</p>	<p>Router# show ip route</p> <p>Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - BGP i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default, U - per-user static route o - ODR, P - periodic downloaded static route</p> <p>Gateway of last resort is not set</p> <p>Cisco IOS IP Routing Protocols Command Reference, Release 12.4 (2005), at IP2R-553</p>	<p>IPv4 Routing Chapter 23 IPv4</p> <p>Examples</p> <ul style="list-style-type: none"> This command displays IP routes learned through BGP. <p>switch#show ip route bgp</p> <pre> Codes: C - connected, S - static, R - kernel, O - OSPF, IA - OSPF inter area, EI - OSPF external type 1, E2 - OSPF external type 2, N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2, I - IGRP, D E - EIGRP, R - RIP, A - Aggregate E E 170.44.43.0/23 [20/0] via 170.44.254.78 E E 170.44.50.0/23 [20/0] via 170.44.254.78 E E 170.44.52.0/23 [20/0] via 170.44.254.78 E E 170.44.54.0/23 [20/0] via 170.44.254.78 E E 170.44.254.112/30 [20/0] via 170.44.254.78 E E 170.52.0.34/32 [1/0] via 170.44.254.2 E I 170.53.0.35/32 [1/0] via 170.44.254.13 via 170.44.254.20 via 170.44.254.67 via 170.44.254.35 via 170.44.254.98 switch# </pre> <p>Arista User Manual v. 4.13.6F (4/14/2014), at 1188.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1039; Arista User Manual, v. 4.11.1 (1/11/13), at 838; Arista User Manual v. 4.10.3 (10/22/12), at 685.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 12.4</p> <p>Effective date of registration: 8/12/2005</p>	<p>Usage Guidelines The <code>clear ip bgp</code> command can be used to initiate a hard reset or soft reconfiguration. A hard reset tears down and rebuilds the specified peering sessions and rebuilds the BGP routing tables. A soft reconfiguration uses stored prefix information to reconfigure and activate BGP routing tables without tearing down existing peering sessions. Soft reconfiguration uses stored update information at the cost of additional memory for storing the updates, to allow you to apply new BGP policy without disrupting the network. Soft reconfiguration can be configured for inbound or outbound sessions.</p> <p>Cisco IOS IP Routing Protocols Command Reference, Release 12.4 (2005), at IRP-69</p>	<p>clear ip bgp</p> <p>The <code>clear ip bgp</code> command removes BGP IPv4 learned routes from the routing table, reads all routes from designated peers, and sends routes to those peers as required.</p> <ul style="list-style-type: none"> a hard reset tears down and rebuilds the peering sessions and rebuilds BGP routing tables. a soft reset uses stored prefix information to reconfigure and activate BGP routing tables without tearing down existing peering sessions. <p>Soft resets use stored update information to apply new BGP policy without disrupting the network. Routes that are read or sent are processed through modified route maps or AS-path access lists. The command can also clear the switch's BGP sessions with its peers.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1577.</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 1527; Arista User Manual v. 4.12.3 (7/17/13), at 1358; Arista User Manual, v. 4.11.1 (1/11/13), at 1104; Arista User Manual v. 4.10.3 (10/22/12), at 916; Arista User Manual v. 4.9.3.2 (5/3/12), at 683; Arista User Manual v. 4.8.2 (11/18/11), at 513; Arista User Manual v. 4.7.3 (7/18/11), at 378.</p>
<p>Cisco IOS 12.4</p> <p>Effective date of registration: 8/12/2005</p>	<p>max-metric router-lsa</p> <p>To configure a router that is running the Open Shortest Path First (OSPF) protocol to advertise a maximum metric so that other routers do not prefer the router as an intermediate hop in their shortest path first (SPF) calculations, use the <code>max-metric router-lsa</code> command in router configuration mode. To disable the advertisement of a maximum metric, use the <code>no</code> form of this command.</p> <pre>max-metric router-lsa [on-startup {seconds wait-for-bgp}] no max-metric router-lsa [on-startup {seconds wait-for-bgp}]</pre> <p>Cisco IOS IP Routing Protocols Command Reference, Release 12.4 (2005), at IP2R-591</p>	<p>Chapter 25 Open Shortest Path First – Version 2 OSPFv2 Commands</p> <p>max-metric router-lsa (OSPFv2)</p> <p>The <code>max-metric router-lsa</code> command allows the OSPF protocol to advertise a maximum metric so that other routers do not prefer the router as an intermediate hop in their SPF calculations.</p> <p>The <code>no max-metric router-lsa</code> and default <code>max-metric router-lsa</code> commands disable the advertisement of a maximum metric.</p> <p>Platform all Command Mode Router-OSPF Configuration</p> <p>Command Syntax</p> <pre>max-metric router-lsa [EXTERNAL] [STUB] [STARTUP] [SUMMARY] no max-metric router-lsa [EXTERNAL] [STUB] [STARTUP] [SUMMARY] default max-metric router-lsa [EXTERNAL] [STUB] [STARTUP] [SUMMARY]</pre> <p>All parameters can be placed in any order.</p> <p>Arista User Manual v. 4.13.6F (4/14/2014), at 1389.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 12.4</p> <p>Effective date of registration: 8/12/2005</p>	<p>adv-router [ip-address]</p> <p>(Optional) Displays all the LSAs of the specified router. If no IP address is included, the information is about the local router itself (in this case, the same as self-originate).</p> <p>link-state-id</p> <p>(Optional) Portion of the Internet environment that is being described by the advertisement. The value entered depends on the advertisement's LS type. It must be entered in the form of an IP address.</p> <p>When the link state advertisement is describing a network, the <i>link-state-id</i> can take one of two forms:</p> <p>The network's IP address (as in type 3 summary link advertisements and in autonomous system external link advertisements).</p> <p>A derived address obtained from the link state ID. (Note that masking a network links advertisement's link state ID with the network's subnet mask yields the network's IP address.)</p> <p>When the link state advertisement is describing a router, the link state ID is always the described router's OSPF router ID.</p> <p>When an autonomous system external advertisement (LS Type = 5) is describing a default route, its link state ID is set to Default Destination (0.0.0.0).</p> <p>Cisco IOS IP Routing Protocols Command Reference, Release 12.4 (2005), at IP2R-613</p>	<p>• linkstate_id Network segment described by the LSA (dotted decimal notation). Value depends on the LSA type.</p> <p>— When the LSA describes a network, the <i>linkstate-id</i> argument is one of the following:</p> <p>The network IP address, as in Type 3 summary link advertisements and in autonomous system external link advertisements.</p> <p>A derived address obtained from the link state ID. Masking a network links the advertisement link state ID with the network subnet mask yielding the network IP address.</p> <p>— When the LSA describes a router, the link state ID is the OSPFv2 router ID of the router.</p> <p>— When an autonomous system external advertisement (Type 5) describes a default route, its link state ID is set to the default destination (0.0.0.0).</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1454.</p> <p><i>See also</i> Arista User Manual v. 4.13.6F (4/14/2014), at 1404; Arista User Manual v. 4.12.3 (7/17/13), at 1240; Arista User Manual, v. 4.11.1 (1/11/13), at 996; Arista User Manual v. 4.10.3 (10/22/12), at 825; Arista User Manual v. 4.9.3.2 (5/3/12), at 648; Arista User Manual v. 4.8.2 (11/18/11), at 483; Arista User Manual v. 4.7.3 (7/18/11), at 357; Arista User Manual v. 4.6.0 (12/22/2010), at 217.</p>

Copyright Registration Information	Cisco	Arista																
Cisco XE 3.5 Effective date of registration: 11/24/2014	<div>area nssa translate</div> <p>To configure a not-so-stubby area (NSSA) and to configure the OSPF Forwarding Address Suppression in Translated Type-5 LSAs feature, use the <code>area nssa translate</code> command in router address family topology or router configuration mode. To remove the NSSA distinction from the area, use the <code>no</code> form of this command.</p> <pre>area nssa translate command area area-id nssa translate type7 [always] suppress-fa] [default-information-originate [metric ospf-metric] [metric-type ospf-link-state-type] [nssa-only]] [no-ext-capability] [no-redistribution] [no-summary] no area area-id nssa translate type7 [always] [suppress-fa] [default-information-originate [metric ospf-metric] [metric-type ospf-link-state-type] [nssa-only]] [no-ext-capability] [no-redistribution] [no-summary]</pre> <table><tr><th>Syntax Description</th><td><code>area-id</code></td><td>Identifier for the stub area or NSSA. The identifier can be specified as either a decimal value or an IP address.</td></tr><tr><td><code>translate</code></td><td></td><td>Translates one type of link-state advertisement (LSA) to another type of LSA. This keyword takes effect only on an NSSA Area Border Router (ABR) or an NSSA Autonomous System Boundary Router (ASBR).</td></tr><tr><td><code>type7</code></td><td></td><td>(Required) Translates a Type-7 LSA to a Type-5 LSA. This keyword takes effect only on an NSSA ABR or an NSSA ASBR.</td></tr><tr><td><code>always</code></td><td></td><td>(Optional) Configures an NSSA ABR router as a forced NSSA LSA translator. The NSSA ABR router unconditionally translates Type-7 LSAs to Type-5 LSAs. You can configure the <code>always</code> keyword only in router configuration mode, not in router address family topology configuration mode.</td></tr></table> <p>Cisco IOS IP Routing: OSPF Command Reference (2011), at 15</p>	Syntax Description	<code>area-id</code>	Identifier for the stub area or NSSA. The identifier can be specified as either a decimal value or an IP address.	<code>translate</code>		Translates one type of link-state advertisement (LSA) to another type of LSA. This keyword takes effect only on an NSSA Area Border Router (ABR) or an NSSA Autonomous System Boundary Router (ASBR).	<code>type7</code>		(Required) Translates a Type-7 LSA to a Type-5 LSA. This keyword takes effect only on an NSSA ABR or an NSSA ASBR.	<code>always</code>		(Optional) Configures an NSSA ABR router as a forced NSSA LSA translator. The NSSA ABR router unconditionally translates Type-7 LSAs to Type-5 LSAs. You can configure the <code>always</code> keyword only in router configuration mode, not in router address family topology configuration mode.	<div>Chapter 26 Open Shortest Path First – Version 3</div> <div>OSPFv3 Commands</div> <div>area nssa translate type7 always (OSPFv3)</div> <p>The <code>area nssa translate type7 always</code> command translates Type-7 link-state advertisement (LSA) to Type-5 of LSAs.</p> <p>The <code>no area nssa translate type7 always</code> command removes the NSSA distinction from the area.</p> <table><tr><td>Platform</td><td>all</td></tr><tr><td>Command Mode</td><td>Router-OSPF3 Configuration</td></tr></table> <p>Command Syntax</p> <pre>area area_id nssa translate type7 always no area_id nssa translate type7 always default area_id nssa translate type7 always</pre> <p>Parameters</p> <ul style="list-style-type: none"><code>area_id</code> area number. <p>Valid formats: integer <1 to 4294967295> or dotted decimal <0.0.0.1 to 255.255.255.255> Area 0 (or 0.0.0.0) is not configurable; it is always <i>normal</i>. <i>Running-config</i> stores value in dotted decimal notation.</p> <p>Example</p> <ul style="list-style-type: none">This command configures an NSSA ABR router as a forced NSSA LSA translator. The NSSA ABR router unconditionally translates Type-7 LSAs to Type-5 LSAs. <pre>switch(config)#ipv6 router ospf 3 switch(config-router-ospf3)#area 3 nssa translate type7 always switch(config-router-ospf3)#</pre> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1501.</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 1451; Arista User Manual v. 4.12.3 (7/17/13), at 1286; Arista User Manual, v. 4.11.1 (1/11/13), at 1036.</p>	Platform	all	Command Mode	Router-OSPF3 Configuration
	Syntax Description	<code>area-id</code>	Identifier for the stub area or NSSA. The identifier can be specified as either a decimal value or an IP address.															
<code>translate</code>		Translates one type of link-state advertisement (LSA) to another type of LSA. This keyword takes effect only on an NSSA Area Border Router (ABR) or an NSSA Autonomous System Boundary Router (ASBR).																
<code>type7</code>		(Required) Translates a Type-7 LSA to a Type-5 LSA. This keyword takes effect only on an NSSA ABR or an NSSA ASBR.																
<code>always</code>		(Optional) Configures an NSSA ABR router as a forced NSSA LSA translator. The NSSA ABR router unconditionally translates Type-7 LSAs to Type-5 LSAs. You can configure the <code>always</code> keyword only in router configuration mode, not in router address family topology configuration mode.																
Platform	all																	
Command Mode	Router-OSPF3 Configuration																	

Copyright Registration Information	Cisco	Arista												
Cisco IOS 12.4 Effective date of registration: 8/12/2005	<div>timers basic (RIP)</div> <p>To adjust Routing Information Protocol (RIP) network timers, use the <code>timers basic</code> command in router configuration mode. To restore the default timers, use the <code>no</code> form of this command.</p> <p><code>timers basic update invalid holddown flush</code></p> <p><code>no timers basic</code></p> <table><tr><td>Syntax Description</td><td><i>update</i></td><td>Rate (in seconds) at which updates are sent. This is the fundamental timing parameter of the routing protocol. The default is 30 seconds.</td></tr><tr><td></td><td><i>invalid</i></td><td>Interval of time (in seconds) after which a route is declared invalid, it should be at least three times the value of the <i>update</i> argument. A route becomes invalid when there is an absence of updates that refresh the route. The route then enters into a <i>holddown</i> state. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets. The default is 90 seconds.</td></tr><tr><td></td><td><i>holddown</i></td><td>Interval (in seconds) during which routing information regarding better paths is suppressed. It should be at least three times the value of the <i>update</i> argument. A route enters into a <i>holddown</i> state when an update packet is received that indicates the route is unreachable. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets. When holddown expires, routes advertised by other sources are accepted and the route is no longer inaccessible. The default is 180 seconds.</td></tr><tr><td></td><td><i>flush</i></td><td>Amount of time (in seconds) that must pass before the route is removed from the routing table; the interval specified should be greater than the value of the <i>invalid</i> argument. If it is less than this sum, the proper <i>holddown</i> interval cannot elapse, which results in a new route being accepted before the <i>holddown</i> interval expires. The default is 240 seconds.</td></tr></table>	Syntax Description	<i>update</i>	Rate (in seconds) at which updates are sent. This is the fundamental timing parameter of the routing protocol. The default is 30 seconds.		<i>invalid</i>	Interval of time (in seconds) after which a route is declared invalid, it should be at least three times the value of the <i>update</i> argument. A route becomes invalid when there is an absence of updates that refresh the route. The route then enters into a <i>holddown</i> state. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets. The default is 90 seconds.		<i>holddown</i>	Interval (in seconds) during which routing information regarding better paths is suppressed. It should be at least three times the value of the <i>update</i> argument. A route enters into a <i>holddown</i> state when an update packet is received that indicates the route is unreachable. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets. When holddown expires, routes advertised by other sources are accepted and the route is no longer inaccessible. The default is 180 seconds.		<i>flush</i>	Amount of time (in seconds) that must pass before the route is removed from the routing table; the interval specified should be greater than the value of the <i>invalid</i> argument. If it is less than this sum, the proper <i>holddown</i> interval cannot elapse, which results in a new route being accepted before the <i>holddown</i> interval expires. The default is 240 seconds.	<div>Chapter 28 Routing Information Protocol<div>timers basic (RIP)</div></div> <div>RIP Commands</div> <p>The <code>timers basic</code> command configures the update interval, the expiration time, and the deletion time for routes received and sent through RIP. The command requires value declaration of all values.</p> <ul style="list-style-type: none">The update time is the interval between unsolicited route responses. The default is 30 seconds.The expiration time is initialized when a route is established and any time an update is received for the route. If the specified period elapses from the last time the route update was received, then the route is marked as inaccessible and advertised as unreachable. However, the route forwards packets until the deletion time expires. The default value is 180 seconds.The deletion time is initialized when the expiration time has elapsed. On initialization of the deletion time, the route is no longer valid; however, it is retained in the routing table for a short time so that neighbors can be notified that the route has been dropped. Upon expiration of the deletion time, the route is removed from the routing table. The default is 120 seconds. <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1671,</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 1621; Arista User Manual v. 4.12.3 (7/17/13), at 1433; Arista User Manual, v. 4.11.1 (1/11/13), at 1179; Arista User Manual v. 4.10.3 (10/22/12), at 989; Arista User Manual v. 4.9.3.2 (5/3/12), at 748; Arista User Manual v. 4.8.2 at 570.</p>
	Syntax Description	<i>update</i>	Rate (in seconds) at which updates are sent. This is the fundamental timing parameter of the routing protocol. The default is 30 seconds.											
	<i>invalid</i>	Interval of time (in seconds) after which a route is declared invalid, it should be at least three times the value of the <i>update</i> argument. A route becomes invalid when there is an absence of updates that refresh the route. The route then enters into a <i>holddown</i> state. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets. The default is 90 seconds.												
	<i>holddown</i>	Interval (in seconds) during which routing information regarding better paths is suppressed. It should be at least three times the value of the <i>update</i> argument. A route enters into a <i>holddown</i> state when an update packet is received that indicates the route is unreachable. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets. When holddown expires, routes advertised by other sources are accepted and the route is no longer inaccessible. The default is 180 seconds.												
	<i>flush</i>	Amount of time (in seconds) that must pass before the route is removed from the routing table; the interval specified should be greater than the value of the <i>invalid</i> argument. If it is less than this sum, the proper <i>holddown</i> interval cannot elapse, which results in a new route being accepted before the <i>holddown</i> interval expires. The default is 240 seconds.												

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 15.2</p> <p>Effective date of registration:</p> <p>11/24/2014</p>	<p>SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response protocol data unit (PDU). If the sender never receives the response, the inform request can be sent again. Thus, informs are more likely than traps to reach their intended destination.</p> <p>Compared to traps, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Also, traps are sent only once; an inform may be tried several times. The retries increase traffic and contribute to a higher overhead on the network.</p> <p>If you do not enter an snmp-server host command, no notifications are sent. To configure the router to send SNMP notifications, you must enter at least one snmp-server host command. If you enter the command with no optional keywords, all trap types are enabled for the host.</p> <p>To enable multiple hosts, you must issue a separate snmp-server host command for each host. You can specify multiple notification types in the command for each host.</p> <p>Cisco IOS IP Switching Command Reference (2011), v. 15.2, at 542</p>	<p>37.2.2 SNMP Notifications</p> <p>SNMP notifications are messages, sent by the agent, to inform managers of an event or a network condition. A <i>trap</i> is an unsolicited notification. An <i>inform</i> (or inform request) is a trap that includes a request for a confirmation that the message is received. Events that a notification can indicate include improper user authentication, restart, and connection losses.</p> <p>Traps are less reliable than informs because the receiver does not send any acknowledgment. However, traps are often preferred because informs consume more switch and network resources. A trap is sent only once and is discarded as soon as it is sent. An inform request remains in memory until a response is received or the request times out. An inform may be retried several times, increasing traffic and contributing to higher network overhead.</p> <p>Table 37-2 lists the SNMP traps that the switch supports.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1963.</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 1891; Arista User Manual v. 4.12.3 (7/17/13), at 1653; Arista User Manual, v. 4.11.1 (1/11/13), at 1341; Arista User Manual v. 4.10.3 (10/22/12), at 1107; Arista User Manual v. 4.9.3.2 (5/3/12), at 863; Arista User Manual v. 4.8.2 at 675; Arista User Manual v. 4.7.3 (7/18/11), at 531.</p>
<p>Cisco IOS 12.4</p> <p>Effective date of registration:</p> <p>8/12/2005</p>	<p>SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response protocol data unit (PDU). If the sender never receives the response, the inform request can be sent again. Thus, informs are more likely than traps to reach their intended destination.</p> <p>Compared to traps, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Also, traps are sent only once; an inform may be tried several times. The retries increase traffic and contribute to a higher overhead on the network.</p> <p>Cisco IOS Network Management Command Reference (2005), at 522</p>	<p>37.2.2 SNMP Notifications</p> <p>SNMP notifications are messages, sent by the agent, to inform managers of an event or a network condition. A <i>trap</i> is an unsolicited notification. An <i>inform</i> (or inform request) is a trap that includes a request for a confirmation that the message is received. Events that a notification can indicate include improper user authentication, restart, and connection losses.</p> <p>Traps are less reliable than informs because the receiver does not send any acknowledgment. However, traps are often preferred because informs consume more switch and network resources. A trap is sent only once and is discarded as soon as it is sent. An inform request remains in memory until a response is received or the request times out. An inform may be retried several times, increasing traffic and contributing to higher network overhead.</p> <p>Table 37-2 lists the SNMP traps that the switch supports.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1963.</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 1891; Arista User Manual v. 4.12.3 (7/17/13), at 1653; Arista User Manual, v. 4.11.1 (1/11/13), at 1341; Arista User Manual v. 4.10.3 (10/22/12), at 1107; Arista User Manual v. 4.9.3.2 (5/3/12), at 863; Arista User Manual v. 4.8.2 at 675; Arista User Manual v. 4.7.3 (7/18/11), at 531.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS XE 3.5</p> <p>Effective date of registration: 11/24/2014</p>	<p>Compared to traps, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Also, traps are sent only once; an inform may be tried several times. The retries increase traffic and contribute to a higher overhead on the network.</p> <p>Cisco IOS IP Switching Command Reference (2011), v. XE 3.5, at 544.</p>	<p>SNMP notifications are messages, sent by the agent, to inform managers of an event or a network condition. A <i>trap</i> is an unsolicited notification. An <i>inform</i> (or inform request) is a trap that includes a request for a confirmation that the message is received. Events that a notification can indicate include improper user authentication, restart, and connection losses.</p> <p>Traps are less reliable than informs because the receiver does not send any acknowledgment. However, traps are often preferred because informs consume more switch and network resources. A trap is sent only once and is discarded as soon as it is sent. An inform request remains in memory until a response is received or the request times out. An inform may be retried several times, increasing traffic and contributing to higher network overhead.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1963.</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 1891; Arista User Manual v. 4.12.3 (7/17/13), at 1653; Arista User Manual, v. 4.11.1 (1/11/13), at 1341; Arista User Manual v. 4.10.3 (10/22/12), at 1107; Arista User Manual v. 4.9.3.2 (5/3/12), at 863; Arista User Manual v. 4.8.2 at 675; Arista User Manual v. 4.7.3 (7/18/11), at 531.</p>
<p>Cisco IOS XE 2.1</p> <p>Effective date of registration: 11/24/2014</p>	<p>Compared to traps, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Also, traps are sent only once; an inform may be tried several times. The retries increase traffic and contribute to a higher overhead on the network.</p> <p>Cisco IOS IP Switching Command Reference (2008), at ISW-344.</p>	<p>SNMP notifications are messages, sent by the agent, to inform managers of an event or a network condition. A <i>trap</i> is an unsolicited notification. An <i>inform</i> (or inform request) is a trap that includes a request for a confirmation that the message is received. Events that a notification can indicate include improper user authentication, restart, and connection losses.</p> <p>Traps are less reliable than informs because the receiver does not send any acknowledgment. However, traps are often preferred because informs consume more switch and network resources. A trap is sent only once and is discarded as soon as it is sent. An inform request remains in memory until a response is received or the request times out. An inform may be retried several times, increasing traffic and contributing to higher network overhead.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1963.</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 1891; Arista User Manual v. 4.12.3 (7/17/13), at 1653; Arista User Manual, v. 4.11.1 (1/11/13), at 1341; Arista User Manual v. 4.10.3 (10/22/12), at 1107; Arista User Manual v. 4.9.3.2 (5/3/12), at 863; Arista User Manual v. 4.8.2 at 675; Arista User Manual v. 4.7.3 (7/18/11), at 531.</p>

Copyright Registration Information	Cisco	Arista												
Cisco IOS 15.2 Effective date of registration: 11/24/2014	<p><i>Table 22 show ip bgp neighbors paths Field Descriptions</i></p> <table><tr><th>Field</th><th>Description</th></tr><tr><td>Address</td><td>Internal address where the path is stored.</td></tr><tr><td>Refcount</td><td>Number of routes using that path.</td></tr></table> <table><tr><th>Field</th><th>Description</th></tr><tr><td>Metric</td><td>Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)</td></tr><tr><td>Path</td><td>Autonomous system path for that route, followed by the origin code for that route.</td></tr></table> <p>Cisco IOS Multiprotocol Label Switching Command Reference (2011), at 640-41.</p>	Field	Description	Address	Internal address where the path is stored.	Refcount	Number of routes using that path.	Field	Description	Metric	Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)	Path	Autonomous system path for that route, followed by the origin code for that route.	<p>show ip bgp paths</p> <p>The show ip bgp paths command displays all BGP paths in the database.</p> <p>Platform all Command Mode EXEC</p> <p>Command Syntax show ip bgp paths [VRF_INSTANCE]</p> <p>Parameters</p> <ul style="list-style-type: none">VRF_INSTANCE specifies VRF instances.<ul style="list-style-type: none"><no parameter> displays routing table for context-active VRF.vrf vrf_name displays routing table for the specified VRF.vrf all displays routing table for all VRFs.vrf default displays routing table for default VRF. <p>Display Values</p> <ul style="list-style-type: none">Refcount: Number of routes using a listed path.Metric: The Multi Exit Discriminator (MED) metric for the path.Path: The autonomous system path for that route, followed by the origin code for that route. <p>The MED, also known as the external metric of a route, provides information to external neighbors about the preferred path into an AS with multiple entry points. Lower MED values are preferred.</p>
	Field	Description												
	Address	Internal address where the path is stored.												
Refcount	Number of routes using that path.													
Field	Description													
Metric	Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)													
Path	Autonomous system path for that route, followed by the origin code for that route.													
	<p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1638.</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 1588; Arista User Manual v. 4.12.3 (7/17/13), at 1405; Arista User Manual, v. 4.11.1 (1/11/13), at 1151; Arista User Manual v. 4.10.3 (10/22/12), at 962; Arista User Manual v. 4.9.3.2 (5/3/12), at 776; Arista User Manual v. 4.8.2 at 547; Arista User Manual v. 4.7.3 (7/18/11), at 401; Arista User Manual v. 4.6.0 (12/22/2010), at 249.</p>													

Copyright Registration Information	Cisco	Arista										
Cisco IOS XE 2.1 Effective date of registration: 11/24/2014	<p>Table 28 <i>show ip bgp neighbors paths Field Descriptions</i></p> <table><tr><th>Field</th><th>Description</th></tr><tr><td>Address</td><td>Internal address where the path is stored.</td></tr><tr><td>Refcount</td><td>Number of routes using that path.</td></tr><tr><td>Metric</td><td>Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)</td></tr><tr><td>Path</td><td>Autonomous system path for that route, followed by the origin code for that route.</td></tr></table> <p>Cisco IOS Multiprotocol Label Switching Command Reference (2008), at 475.</p>	Field	Description	Address	Internal address where the path is stored.	Refcount	Number of routes using that path.	Metric	Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)	Path	Autonomous system path for that route, followed by the origin code for that route.	<p>show ip bgp paths</p> <p>The show ip bgp paths command displays all BGP paths in the database.</p> <p>Platform all Command Mode EXEC</p> <p>Command Syntax</p> <p>show ip bgp paths [VRF_INSTANCE]</p> <p>Parameters</p> <ul style="list-style-type: none">• VRF_INSTANCE specifies VRF instances.<ul style="list-style-type: none">— <no parameter> displays routing table for context-active VRE— vrf vrf_name displays routing table for the specified VRF.— vrf all displays routing table for all VRFs.— vrf default displays routing table for default VRF <p>Display Values</p> <ul style="list-style-type: none">• Refcount: Number of routes using a listed path.• Metric: The Multi Exit Discriminator (MED) metric for the path.• Path: The autonomous system path for that route, followed by the origin code for that route. <p>The MED, also known as the external metric of a route, provides information to external neighbors about the preferred path into an AS with multiple entry points. Lower MED values are preferred.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1638.</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 1588; Arista User Manual v. 4.12.3 (7/17/13), at 1405; Arista User Manual, v. 4.11.1 (1/11/13), at 1151; Arista User Manual v. 4.10.3 (10/22/12), at 962; Arista User Manual v. 4.9.3.2 (5/3/12), at 776; Arista User Manual v. 4.8.2 at 547; Arista User Manual v. 4.7.3 (7/18/11), at 401; Arista User Manual v. 4.6.0 (12/22/2010), at 249</p>
	Field	Description										
	Address	Internal address where the path is stored.										
	Refcount	Number of routes using that path.										
	Metric	Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)										
Path	Autonomous system path for that route, followed by the origin code for that route.											

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 15.2</p> <p>Effective date of registration:</p> <p>11/24/2014</p>	<p>Usage Guidelines</p> <p>This command configures the HTTP server to request an X.509v3 certificate from the client in order to authenticate the client during the connection process.</p> <p>In the default connection and authentication process, the client requests a certificate from the HTTP server, but the server does not attempt to authenticate the client. Authenticating the client provides more security than server authentication by itself, but not all web clients may be configured for certificate authority (CA) authentication.</p> <p>Cisco IOS HTTP Services Configuration Guide (2011), at 49.</p>	<p>protocol https certificate (API Management)</p> <p>The protocol <code>https certificate</code> command configures the HTTP secure server to request an X.509 certificate from the client to configure the server certificate. The client (usually a web browser), in turn, has a public key that allows it to authenticate the certificate.</p> <p>The <code>no protocol https certificate</code> and <code>default protocol https certificate</code> commands restore default behavior by removing the protocol <code>https certificate</code> statement from <i>running-config</i>.</p> <p>Platform all Command Mode Mgmt-api Configuration</p> <p>Command Syntax</p> <pre>protocol https certificate no protocol https certificate default protocol https certificate</pre> <p>Related Commands</p> <ul style="list-style-type: none"> <code>management api http-commands</code> places the switch in Management-api configuration mode. <p>Examples</p> <ul style="list-style-type: none"> These commands configure the HTTP server to request an X.509 certificate from the client in order to authenticate the client during the connection process. <pre>switch(config)#management api http-commands switch(config-mgmt-api-http-cmds)#protocol https certificate switch(config-mgmt-api-http-cmds)#</pre> <p>Arista User Manual v. 4.13.6F (4/14/2014), at 85.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 75.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 15.2</p> <p>Effective date of registration:</p> <p>11/24/2014</p>	<p>Usage Guidelines To configure a remote user, specify the IP address or port number for the remote SNMP agent of the device where the user resides. Also, before you configure remote users for a particular agent, configure the SNMP engine ID, using the <code>snmp-server engineID</code> command with the <code>remote</code> keyword. The remote agent's</p> <p>Cisco IOS SNMP Support Command Reference (2011), at 380</p>	<p>Configuring the Group</p> <p>An SNMP group is a table that maps SNMP users to SNMP views. The <code>snmp-server group</code> command configures a new SNMP group.</p> <p>Example</p> <ul style="list-style-type: none"> This command configures <code>normal_one</code> as an SNMPv3 group (authentication and encryption) that provides access to the <code>all-items</code> read view. <pre>switch(config)#snmp-server group normal_one v3 priv read all-items switch(config)#</pre> <p>Configuring the User</p> <p>An SNMP user is a member of an SNMP group. The <code>snmp-server user</code> command adds a new user to an SNMP group and configures that user's parameters. To configure a remote user, specify the IP address or port number of the device where the user's remote SNMP agent resides.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1966.</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 1894; Arista User Manual v. 4.12.3 (7/17/13), at 1656; Arista User Manual, v. 4.11.1 (1/11/13), at 1344; Arista User Manual v. 4.10.3 (10/22/12), at 1110; Arista User Manual v. 4.9.3.2 (5/3/12), at 865; Arista User Manual v. 4.8.2 (11/18/11), at 677; Arista User Manual v. 4.7.3 (7/18/11), at 533.</p>

Copyright Registration Information	Cisco	Arista														
Cisco IOS 15.2 Effective date of registration: 11/24/2014	<p>Usage Guidelines</p> <p>The <code>show snmp host</code> command displays details such as IP address of the Network Management System (NMS), notification type, SNMP version, and the port number of the NMS.</p> <p>To configure these details, use the <code>snmp-server host</code> command.</p> <p>Command Examples</p> <p>The following is sample output from the <code>show snmp host</code> command.</p> <pre>Router# show snmp host Notification host: 10.2.20.6 udp-port: 162 type: inform user: public security model: v3c traps: 00001000.00000000.00000000</pre> <p>The table below describes the significant fields shown in the display.</p> <p>Table 5 <i>show snmp host</i> Field Descriptions</p> <table><tr><th>Field</th><th>Description</th></tr><tr><td>Notification host</td><td>Displays the IP address of the host for which the notification is generated.</td></tr><tr><td>udp-port</td><td>Displays the port number.</td></tr><tr><td>type</td><td>Displays the type of notification.</td></tr><tr><td>user</td><td>Displays the access type of the user for which the notification is generated.</td></tr><tr><td>security model</td><td>Displays the SNMP version used to send notifications.</td></tr><tr><td>traps</td><td>Displays details of the notification generated.</td></tr></table> <p>Cisco IOS SNMP Support Command Reference (July 2011), at 108–09</p>	Field	Description	Notification host	Displays the IP address of the host for which the notification is generated.	udp-port	Displays the port number.	type	Displays the type of notification.	user	Displays the access type of the user for which the notification is generated.	security model	Displays the SNMP version used to send notifications.	traps	Displays details of the notification generated.	<p>SNMP Commands Chapter 37 SNMP</p> <p>show snmp host</p> <p>The <code>show snmp host</code> command displays the recipient details for Simple Network Management Protocol (SNMP) notification operations. Details that the command displays include IP address and port number of the Network Management System (NMS), notification type, and SNMP version.</p> <p>Platform all Command Mode EXEC</p> <p>Command Syntax</p> <pre>show snmp host</pre> <p>Field Descriptions</p> <ul style="list-style-type: none">• Notification host IP address of the host for which the notification is generated.• udp-port port number.• type notification type.• user access type of the user for which the notification is generated.• security model SNMP version used to send notifications.• traps details of the notification generated. <p>Arista User Manual v. 4.13.6F (4/14/2014), at 1908</p> <p><i>See also</i> Arista User Manual v.4.14.3F (Rev. 2) (10/2/2014), at 1980; Arista User Manual v. 4.12.3 (7/17/13), at 1670; Arista User Manual, v. 4.11.1 (1/11/13), at 1357; Arista User Manual v. 4.10.3 (10/22/12), at 1124; Arista User Manual v. 4.9.3.2 (5/3/12), at 880; Arista User Manual v. 4.8.2 (11/18/11), at 688; Arista User Manual v. 4.7.3 (7/18/11), at 544.</p>
	Field	Description														
	Notification host	Displays the IP address of the host for which the notification is generated.														
	udp-port	Displays the port number.														
	type	Displays the type of notification.														
user	Displays the access type of the user for which the notification is generated.															
security model	Displays the SNMP version used to send notifications.															
traps	Displays details of the notification generated.															

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 15.2</p> <p>Effective date of registration:</p> <p>11/24/2014</p>	<p>show snmp view</p> <p>To display the family name, storage type, and status of a Simple Network Management Protocol (SNMP) configuration and associated MIB, use the show snmp view command in privileged EXEC mode.</p> <p>Cisco IOS SNMP Support Command Reference (2011), at 140</p>	<p>SNMP Commands Chapter 37 SNMP</p> <p>show snmp view</p> <p>The show snmp view command displays the family name, storage type, and status of a Simple Network Management Protocol (SNMP) configuration and the associated MIB. SNMP views are configured with the snmp-server view command.</p> <p>Platform all Command Mode EXEC</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1986.</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 1914; Arista User Manual v. 4.12.3 (7/17/13), at 1676; Arista User Manual, v. 4.11.1 (1/11/13), at 1361; Arista User Manual v. 4.10.3 (10/22/12), at 1128; Arista User Manual v. 4.9.3.2 (5/3/12), at 884; Arista User Manual v. 4.8.2 (11/18/11), at 692; Arista User Manual v. 4.7.3 (7/18/11), at 548.</p>
<p>Cisco IOS 15.2</p> <p>Effective date of registration:</p> <p>11/24/2014</p>	<p>Usage Guidelines This command provides counter information for SNMP operations. It also displays the chassis ID string defined with the snmp-server chassis-id global configuration command.</p> <p>Command Examples The following is sample output from the show snmp command:</p> <pre> Router# show snmp Chassis: 12161081 0 SNMP packets input 0 Bad SNMP version errors 0 Unknown community name 0 Illegal operation for community name supplied 0 Encoding errors 0 Number of requested variables 0 Number of altered variables 0 Get-request PDUs 0 Get-next PDUs 0 Set-request PDUs 0 Input queue packet drops (Maximum queue size 1000) 0 SNMP packets output 0 Too big errors (Maximum packet size 1500) 0 No such name errors 0 Bad value errors 0 General errors 0 Response PDUs 0 Trap PDUs SNMP logging: enabled </pre> <p>Cisco IOS SNMP Support Command Reference (2011), at 95-96</p>	<p>Configuring SNMP Chapter 37 SNMP</p> <pre> 8 SNMP packets input 0 Bad SNMP version errors 0 Unknown community name 0 Illegal operation for community name supplied 0 Encoding errors 8 Number of requested variables 0 Number of altered variables 4 Get-request PDUs 4 Get-next PDUs 0 Set-request PDUs 11 SNMP packets output 0 Too big errors 0 No such name errors 0 Bad value errors 0 General errors 8 Response PDUs 0 Trap PDUs SNMP logging: enabled Logging to taccom.log SNMP agent enabled switch(config)# </pre> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1967-68.</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 1896; Arista User Manual v. 4.12.3 (7/17/13), at 1658; Arista User Manual, v. 4.11.1 (1/11/13), at 1345; Arista User Manual v. 4.10.3 (10/22/12), at 1091; Arista User Manual v. 4.9.3.2 (5/3/12), at 868; Arista User Manual v. 4.8.2 (11/18/11), at 678; Arista User Manual v. 4.7.3 (7/18/11), at 534.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 15.2</p> <p>Effective date of registration:</p> <p>11/24/2014</p>	<p><code>snmp-server engineID local</code></p> <p><code>snmp-server engineID local through snmp trap link-status</code></p> <p>and the local engine ID. The command line password is then destroyed, as required by RFC 2274. Because of this deletion, if the local value of engineID changes, the security digests of SNMPv3 users will be invalid, and the users will have to be reconfigured.</p> <p>Similar restrictions require the reconfiguration of community strings when the engine ID changes. A remote engine ID is required when an SNMPv3 inform is configured. The remote engine ID is used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host.</p> <p>Cisco IOS SNMP Support Command Reference (2011), at 324.</p>	<p><code>snmp-server engineID remote</code></p> <p>The <code>snmp-server engineID remote</code> command configures the name of a Simple Network Management Protocol (SNMP) engine located on a remote device. The switch generates a default engineID; use the <code>show snmp engineID</code> command to view the configured or default engineID.</p> <p>A remote engine ID is required when configuring an SNMPv3 inform to compute the security digest for authenticating and encrypting packets sent to users on the remote host. SNMPv3 authenticates users through security digests (MD5 or SHA) that are based on user passwords and the engine ID. Passwords entered on the CLI are similarly converted, then compared to the user's security digest to authenticate the user.</p> <p>Arista User Manual v. 4.13.6F (4/14/2014), at 1920.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1682; Arista User Manual, v. 4.11.1 (1/11/13), at 1367; Arista User Manual v. 4.10.3 (10/22/12), at 1134; Arista User Manual v. 4.9.3.2 (5/3/12), at 890; Arista User Manual v. 4.8.2 (11/18/11), at 698; Arista User Manual v. 4.7.3 (7/18/11), at 554.</p>
<p>Cisco IOS 12.4</p> <p>Effective date of registration:</p> <p>8/12/2005</p>	<p><code>aaa group server radius</code></p> <p>To group different RADIUS server hosts into distinct lists and distinct methods, enter the <code>aaa group server radius</code> command in global configuration mode. To remove a group server from the configuration list, enter the <code>no</code> form of this command.</p> <p><code>aaa group server radius group-name</code></p> <p><code>no aaa group server radius group-name</code></p> <p>Cisco IOS Security Command Reference, Release 12.4 (2005), at SEC-74.</p>	<p><code>aaa group server radius</code></p> <p>The <code>aaa group server radius</code> command enters the server-group-radius configuration mode for the specified group name. The command creates the specified group if it was not previously created. Commands are available to add servers to the group.</p> <p>A server group is a collection of servers that are associated with a single label. Subsequent authorization and authentication commands access all servers in a group by invoking the group name. Server group members must be previously configured with a <code>radius-server host</code> command.</p> <p>The <code>no aaa group server radius</code> and default <code>aaa group server radius</code> commands delete the specified server group from <i>running-config</i>.</p> <p>Platform all Command Mode Global Configuration</p> <p>Command Syntax</p> <p><code>aaa group server radius group_name</code></p> <p><code>no aaa group server radius group_name</code></p> <p><code>default aaa group server radius group_name</code></p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 224.</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 217; Arista User Manual v. 4.12.3 (7/17/13), at 168; Arista User Manual, v. 4.11.1 (1/11/13), at 126; Arista User Manual v. 4.10.3 (10/22/12), at 118.</p>

Copyright Registration Information	Cisco	Arista									
Cisco IOS 12.4 Effective date of registration: 8/12/2005	<p>aaa authentication dot1x</p> <p>To specify one or more authentication, authorization, and accounting (AAA) methods for use on interfaces running IEEE 802.1X, use the aaa authentication dot1x command in global configuration mode. To disable authentication, use the no form of this command.</p> <p>Cisco IOS Security Command Reference, Release 12.4 (2005), at SEC-32.</p>	<p>11.3.1 Configuring an Authentication Method List for 802.1x</p> <p>To use 802.1x port security, specify an authentication method to be used to authenticate clients. The switch supports RADIUS authentication with 802.1x port security. To use RADIUS authentication with 802.1x port security, you create an authentication method list for 802.1x and specify RADIUS as an authentication method, then configure communication between the switch and RADIUS server.</p> <p>Example</p> <ul style="list-style-type: none">The aaa authentication dot1x command specifies one or more authentication, authorization, and accounting (AAA) methods for use on interfaces running IEEE 802.1X. The following example uses the aaa authentication dot1x command with RADIUS authentication. <pre>switch> enable switch# configure terminal switch(config)# aaa authentication dot1x default group radius</pre> <p>Arista User Manual v. 4.13.6F (4/14/2014), at 551,</p>									
Cisco IOS 12.4 Effective date of registration: 8/12/2005	<p>dot1x port-control</p> <p>To set an 802.1X port control value, use the dot1x port-control command in interface configuration mode. To disable the port-control value, use the no form of this command.</p> <p>dot1x port-control {auto force-authorized force-unauthorized}</p> <p>no dot1x port-control {auto force-authorized force-unauthorized}</p> <table><tr><td>Syntax Description</td><td>auto</td><td>Determines authentication status of the client PC by the authentication process. The port state will be set to AUTO</td></tr><tr><td></td><td>force-authorized</td><td>Disables 802.1X on the interface and causes the port to change to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1X-based authentication of the client. The force-authorized keyword is the default.</td></tr><tr><td></td><td>force-unauthorized</td><td>Denies all access through this interface by forcing the port to change to the unauthorized state, ignoring all attempts by the client to authenticate.</td></tr></table> <p>Cisco IOS Security Command Reference, Release 12.4 (2005), at SEC-457.</p>	Syntax Description	auto	Determines authentication status of the client PC by the authentication process. The port state will be set to AUTO		force-authorized	Disables 802.1X on the interface and causes the port to change to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1X-based authentication of the client. The force-authorized keyword is the default.		force-unauthorized	Denies all access through this interface by forcing the port to change to the unauthorized state, ignoring all attempts by the client to authenticate.	<p>Example</p> <ul style="list-style-type: none">This command configures Ethernet 1 to immediately commence functioning as authenticator ports. <pre>switch(config)#interface ethernet 1 switch(config-if-Et1)#dot1x port-control auto switch(config-if-Et1)#</pre> <p>The dot1x port-control force-authorized command causes the port to transition to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1X-based authentication of the client.</p> <p>Example</p> <ul style="list-style-type: none">This example of the command designates Ethernet 1 as an authenticator port that is to continue to forward packets. <pre>switch(config)#interface ethernet 1 switch(config-if-Et1)#dot1x port-control force-authorized switch(config-if-Et1)#</pre> <p>Example</p> <ul style="list-style-type: none">The dot1x port-control force-unauthorized command places the specified ports in the state of unauthorized, denying any access requests from users of the ports. <pre>switch(config)#interface ethernet 1 switch(config-if-Et1)#dot1x port-control force-unauthorized switch(config-if-Et1)#</pre> <p>Arista User Manual v. 4.13.6F (4/14/2014), at 552,</p>
Syntax Description	auto	Determines authentication status of the client PC by the authentication process. The port state will be set to AUTO									
	force-authorized	Disables 802.1X on the interface and causes the port to change to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1X-based authentication of the client. The force-authorized keyword is the default.									
	force-unauthorized	Denies all access through this interface by forcing the port to change to the unauthorized state, ignoring all attempts by the client to authenticate.									

Copyright Registration Information	Cisco	Arista													
Cisco IOS 15.2 Effective date of registration: 11/24/2014	<div>dot1x max-reauth-req</div> <div>To set the maximum number of times the authenticator sends an Extensible Authentication Protocol (EAP) request/identity frame (assuming that no response is received) to the client, use the dot1x max-reauth-req command in interface configuration mode. To set the maximum number of times to the default setting of 2, use the no form of this command.</div> <div>dot1x max-reauth-req number no dot1x max-reauth-req</div> <div>Cisco IOS Security Command Reference: Commands D to L (2011), at 164.</div>	<div>11.3.5 Setting the Maximum Number of Times the Authenticator Sends EAP Request</div> <div>The dot1x max-reauth-req command sets the maximum number of times that the switch restarts the authentication process before a port changes to the unauthorized state.</div> <div>Example</div> <div><ul style="list-style-type: none">These commands set the maximum number of times the authenticator sends an Extensible Authentication Protocol (EAP) request/identity frame to the client.<pre>switch(config)#interface ethernet 1 switch(config-if-Btl)#dot1x max-reauth-req 4 switch(config-if-Btl)#</pre></div> <div>Arista User Manual v. 4.13.6F (4/14/2014), at 553,</div>													
Cisco IOS 12.4 Effective date of registration: 8/12/2005	<div>dot1x pae</div> <div>To set the Port Access Entity (PAE) type, use the dot1x pae command in interface configuration mode. To disable the PAE type that was set, use the no form of this command.</div> <div>dot1x pae [supplicant authenticator both] no dot1x pae [supplicant authenticator both]</div> <div><table><tr><td>Syntax Description</td><td>supplicant</td><td>(Optional) The interface acts only as a supplicant and will not respond to messages that are meant for an authenticator.</td></tr><tr><td></td><td>authenticator</td><td>(Optional) The interface acts only as an authenticator and will not respond to any messages meant for a supplicant.</td></tr><tr><td></td><td>both</td><td>(Optional) The interface behaves both as a supplicant and as an authenticator and thus will respond to all dot1x messages.</td></tr></table></div> <div>Cisco IOS Security Command Reference, Release 12.4 (2005), at SEC-456.</div>	Syntax Description	supplicant	(Optional) The interface acts only as a supplicant and will not respond to messages that are meant for an authenticator.		authenticator	(Optional) The interface acts only as an authenticator and will not respond to any messages meant for a supplicant.		both	(Optional) The interface behaves both as a supplicant and as an authenticator and thus will respond to all dot1x messages.	<div>dot1x pae authenticator</div> <div>The dot1x pae authenticator command sets the Port Access Entity (PAE) type. The interface acts only as an authenticator and will not respond to any messages meant for a supplicant.</div> <div>The no dot1x pae authenticator and default dot1x pae authenticator commands restore the switch default by deleting the corresponding dot1x pae authenticator command from running-config.</div> <div><table><tr><td>Platform</td><td>all</td></tr><tr><td>Command Mode</td><td>Interface-Ethernet Configuration Interface-Management Configuration</td></tr></table></div> <div>Arista User Manual v. 4.13.6F (4/14/2014), at 560.</div>	Platform	all	Command Mode	Interface-Ethernet Configuration Interface-Management Configuration
Syntax Description	supplicant	(Optional) The interface acts only as a supplicant and will not respond to messages that are meant for an authenticator.													
	authenticator	(Optional) The interface acts only as an authenticator and will not respond to any messages meant for a supplicant.													
	both	(Optional) The interface behaves both as a supplicant and as an authenticator and thus will respond to all dot1x messages.													
Platform	all														
Command Mode	Interface-Ethernet Configuration Interface-Management Configuration														

Copyright Registration Information	Cisco	Arista						
Cisco IOS 12.4 Effective date of registration: 8/12/2005	<p>dot1x timeout (EtherSwitch)</p> <p>To set the number of retry seconds between 802.1X authentication exchanges when an Ethernet switch network module is installed in the router, use the dot1x timeout command in global configuration mode. To return to the default setting, use the no form of this command.</p> <p>dot1x timeout {quiet-period seconds re-authperiod seconds tx-period seconds}</p> <p>no dot1x timeout {quiet-period seconds re-authperiod seconds tx-period seconds}</p> <table><tr><td>Syntax Description</td><td>quiet-period seconds Specifies the time in seconds that the Ethernet switch network module remains in the quiet state following a failed authentication exchange with the client. The range is from 0 to 65535 seconds. The default is 60 seconds</td></tr></table> <p>Cisco IOS Security Command Reference, Release 12.4 (2005), at SEC-466.</p>	Syntax Description	quiet-period seconds Specifies the time in seconds that the Ethernet switch network module remains in the quiet state following a failed authentication exchange with the client. The range is from 0 to 65535 seconds. The default is 60 seconds	<p>dot1x timeout quiet-period</p> <p>The dot1x timeout quiet-period command sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client. The range is 1 to 65535 seconds; the default is 60.</p> <p>When the switch cannot authenticate the client, the switch remains idle for a set period of time and then tries again. You can provide a faster response time to the user by entering a number smaller than the default.</p> <p>The no dot1x timeout quiet-period and default dot1x timeout quiet-period commands restore the default advertisement interval of 60 seconds by removing the corresponding dot1x timeout quiet-period command from <i>running-config</i>.</p> <table><tr><td>Platform</td><td>all</td></tr><tr><td>Command Mode</td><td>Interface-Ethernet Configuration Interface-Management Configuration</td></tr></table> <p>Arista User Manual v. 4.13.6F (4/14/2014), at 563,</p>	Platform	all	Command Mode	Interface-Ethernet Configuration Interface-Management Configuration
	Syntax Description	quiet-period seconds Specifies the time in seconds that the Ethernet switch network module remains in the quiet state following a failed authentication exchange with the client. The range is from 0 to 65535 seconds. The default is 60 seconds						
Platform	all							
Command Mode	Interface-Ethernet Configuration Interface-Management Configuration							
Cisco IOS 12.4 Effective date of registration: 8/12/2005	<p>Usage Guidelines</p> <p>The security passwords min-length command provides enhanced security access to the router by allowing you to specify a minimum password length, eliminating common passwords that are prevalent on most networks, such as "lab" and "cisco." This command affects user passwords, enable passwords and secrets, and line passwords. After this command is enabled, any password that is less than the specified length will fail.</p> <p>Cisco IOS Security Command Reference, Release 12.4 (2005), at SEC-943.</p>	<p>password minimum length (Security Management)</p> <p>The password minimum length command provides enhanced security access to the switch by allowing you to specify a minimum password length, eliminating common passwords that are prevalent on most networks. This command affects user passwords, enable passwords and secrets, and line passwords. After this command is enabled, any password that is less than the specified length will fail.</p> <p>Applicable CC Requirements: The switch settings for secure passwords can be found under secure preparation. The password minimum length should be 15 characters and SHA-512 should be used as the hashing mechanism for all locally stored passwords.</p> <p>Arista User Manual v. 4.13.6F (4/14/2014), at 152,</p>						

Copyright Registration Information	Cisco	Arista																																								
Cisco IOS 15.2 Effective date of registration: 11/24/2014	<p>Command Examples This example shows the output from the <code>show port-security</code> command when you do not enter any options:</p> <pre>Router# show port-security</pre> <table><thead><tr><th>Secure Port</th><th>MaxSecureAddr</th><th>CurrentAddr</th><th>SecurityViolation</th><th>Security Action</th></tr><tr><th></th><th>(Count)</th><th>(Count)</th><th>(Count)</th><th></th></tr></thead><tbody><tr><td>Fa5/1</td><td>11</td><td>11</td><td>0</td><td>Shutdown</td></tr><tr><td>Fa5/5</td><td>15</td><td>5</td><td>0</td><td>Restrict</td></tr><tr><td>Fa5/11</td><td>5</td><td>4</td><td>0</td><td>Protect</td></tr></tbody></table> <p>-----</p> <p>Total Addresses in System: 21 Max Addresses limit in System: 128 Router#</p> <p>Cisco IOS Security Command Reference Commands S to Z (July 2011), at 692.</p>	Secure Port	MaxSecureAddr	CurrentAddr	SecurityViolation	Security Action		(Count)	(Count)	(Count)		Fa5/1	11	11	0	Shutdown	Fa5/5	15	5	0	Restrict	Fa5/11	5	4	0	Protect	<p>Example</p> <ul style="list-style-type: none">These commands enable MAC security on Ethernet interface 7, set the maximum number of assigned MAC addresses to 2, assigns two static MAC addresses to the interface, and clears the dynamic MAC addresses for the interface. <pre>switch(config)#interface ethernet 7 switch(config-if-Et7)#switchport port-security switch(config-if-Et7)#switchport port-security maximum 2 switch(config-if-Et7)#exit switch(config)#mac address-table static 0034.24c2.8f11 vlan 10 interface ethernet 7 switch(config)#mac address-table static 4464.942d.17ce vlan 10 interface ethernet 7 switch(config)#clear mac address-table dynamic interface ethernet 7 switch(config)#show port-security</pre> <table><thead><tr><th>Secure Port</th><th>MaxSecureAddr</th><th>CurrentAddr</th><th>SecurityViolation</th><th>Security Action</th></tr><tr><th></th><th>(Count)</th><th>(Count)</th><th>(Count)</th><th></th></tr></thead><tbody><tr><td>Et7</td><td>2</td><td>2</td><td>0</td><td>Shutdown</td></tr></tbody></table> <p>-----</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 632.</p> <p><i>See also</i> Arista User Manual v. 4.13.6F (4/14/2014), at 624; Arista User Manual v. 4.12.3 (7/17/13), at 501; Arista User Manual, v. 4.11.1 (1/11/13), at 405-06; Arista User Manual v. 4.10.3 (10/22/12), at 336.</p>	Secure Port	MaxSecureAddr	CurrentAddr	SecurityViolation	Security Action		(Count)	(Count)	(Count)		Et7	2	2	0	Shutdown
	Secure Port	MaxSecureAddr	CurrentAddr	SecurityViolation	Security Action																																					
		(Count)	(Count)	(Count)																																						
Fa5/1	11	11	0	Shutdown																																						
Fa5/5	15	5	0	Restrict																																						
Fa5/11	5	4	0	Protect																																						
Secure Port	MaxSecureAddr	CurrentAddr	SecurityViolation	Security Action																																						
	(Count)	(Count)	(Count)																																							
Et7	2	2	0	Shutdown																																						

Copyright Registration Information	Cisco	Arista				
Cisco IOS XE 3.5 Effective date of registration: 11/24/2014	<div><div>Command Modes</div><div>PTP clock configuration (config-ptp-clk)</div></div> <div><div>Command History</div><table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>15.0(1)S</td><td>This command was introduced.</td></tr></tbody></table></div> <div><div>Usage Guidelines</div><div>Slave devices use the priority1 value when selecting a master clock. The priority1 value has precedence over the priority2 value.</div></div> <div>Cisco IOS Interface and Hardware Component Command Reference (2011), at 1018.</div>	Release	Modification	15.0(1)S	This command was introduced.	<div><div>ptp priority1</div><div>The ptp priority1 command configures the priority1 value to use when advertising the clock. This value overrides the default criteria for best master clock selection. Lower values take precedence. The range is from 0 to 255. To remove PTP settings, use the no form of this command.</div><div><div>Platform</div><div>FM6000</div><div>Command Mode</div><div>Global Configuration</div></div><div><div>Command Syntax</div><div><div>ptp priority1 priority_rate</div><div>no ptp priority1</div><div>default ptp priority1</div></div></div><div><div>Parameters</div><div><ul style="list-style-type: none"><i>priority_rate</i> The value to override the default criteria (clock quality, clock class, etc.) for best master clock selection. Lower values take precedence. Value ranges from 0 to 255. The default is 128.</div></div><div><div>Examples</div><div><ul style="list-style-type: none">This command configures the preference level for a clock. slave devices use the priority1 value when selecting a master clock.</div></div><div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 589.</div><div>See also Arista User Manual v. 4.13.6F (4/14/2014), at 318; Arista User Manual v. 4.12.3 (7/17/13), at 262; Arista User Manual, v. 4.11.1 (1/11/13), at 208.</div></div>
	Release	Modification				
	15.0(1)S	This command was introduced.				

Copyright Registration Information	Cisco	Arista						
<p>Cisco IOS 12.4</p> <p>Effective date of registration: 8/12/2005</p>	<p>service sequence-numbers</p> <p>To enable visible sequence numbering of system logging messages, use the service sequence-numbers command in global configuration mode. To disable visible sequence numbering of logging messages, use the no form of this command.</p> <p>service sequence-numbers</p> <p>no service sequence-numbers</p> <p>Syntax Description This command has no arguments or keywords.</p> <p>Defaults Disabled.</p> <p>Command Modes Global configuration</p> <table border="1"> <thead> <tr> <th>Command History</th><th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td></td><td>12.0</td><td>This command was introduced.</td></tr> </tbody> </table> <p>Usage Guidelines Each system status messages logged in the system logging process have a sequence reference number applied. This command makes that number visible by displaying it with the message. The sequence number is displayed as the first part of the system status message. See the description of the logging commands for information on displaying logging messages.</p> <p>Cisco IOS Configuration Fundamentals Command Reference Release 12.4T (2005), at CF-472.</p>	Command History	Release	Modification		12.0	This command was introduced.	<p>service sequence-numbers</p> <p>The service sequence-numbers command enables visible sequence numbering of system logging messages. Each system status messages logged in the system logging process have a sequence reference number applied. This command makes that number visible by displaying it with the message.</p> <p>The no service sequence-numbers and default service sequence-numbers commands disable visible sequence numbering of system logging messages by removing the service sequence-numbers command from <i>running-config</i>.</p> <p>Arista User Manual v. 4.13.6F (4/14/2014), at 380.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 322; Arista User Manual, v. 4.11.1 (1/11/13), at 268.</p>
Command History	Release	Modification						
	12.0	This command was introduced.						

Copyright Registration Information	Cisco	Arista																		
Cisco IOS 15.1 Effective date of registration: 11/28/2014	<p>Usage Guidelines</p> <p>The command history function provides a record of EXEC commands that you have entered. This function is particularly useful for recalling long or complex commands or entries, including access lists. To change the number of command lines that the system will record in its history buffer, use the history size line configuration command.</p> <p>The history command enables the history function with the last buffer size specified or, if there was not a prior setting, with the default of ten lines. The no history command disables the history function.</p> <p>The show history EXEC command will list the commands you have entered, but you can also use your keyboard to display individual commands. Table 34 lists the keys you can use to recall commands from the command history buffer.</p> <p>Table 34 History Keys</p> <table><tr><th>Key(s)</th><th>Functions</th></tr><tr><td>Ctrl-P or Up Arrow¹</td><td>Recalls commands in the history buffer in a backward sequence, beginning with the most recent command. Repeat the key sequence to recall successively older commands.</td></tr><tr><td>Ctrl-N or Down Arrow¹</td><td>Returns to more recent commands in the history buffer after recalling commands with Ctrl-P or the Up Arrow. Repeat the key sequence to recall successively more recent commands.</td></tr></table> <p><small>1. The arrow keys function only with ANSI-compatible terminals.</small></p> <p>Cisco IOS Configuration Fundamentals Command Reference (2010), at CF-237.</p>	Key(s)	Functions	Ctrl-P or Up Arrow ¹	Recalls commands in the history buffer in a backward sequence, beginning with the most recent command. Repeat the key sequence to recall successively older commands.	Ctrl-N or Down Arrow ¹	Returns to more recent commands in the history buffer after recalling commands with Ctrl-P or the Up Arrow. Repeat the key sequence to recall successively more recent commands.	<p>3.2.4 History Substitution Keystrokes</p> <p>The history buffer retains the last 20 entered commands. History substitution keystrokes that access previously entered commands include:</p> <ul style="list-style-type: none">• Ctrl-P or the Up Arrow key: Recalls history buffer commands, beginning with the most recent command. Repeat the key sequence to recall older commands.• Ctrl-N or the Down Arrow key: Returns to more recent commands after using the Ctrl-P or the Up Arrow. Repeat the key sequence to recall more recent commands. <p>The show history command in Privileged EXEC mode displays the history buffer contents.</p> <pre>switch#show history en config exit show history</pre> <p>Arista User Manual v. 4.13.6F (4/14/2014), at 103.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 93; Arista User Manual, v. 4.11.1 (1/11/13), at 63; Arista User Manual v. 4.10.3 (10/22/12), at 55; Arista User Manual v. 4.9.3.2 (5/3/12), at 51; Arista User Manual v. 4.8.2 (11/18/11), at 47; Arista User Manual v. 4.7.3 (7/18/11), at 44-45; Arista User Manual v. 4.6.0 (12/22/2010), at 38-39</p>												
Key(s)	Functions																			
Ctrl-P or Up Arrow ¹	Recalls commands in the history buffer in a backward sequence, beginning with the most recent command. Repeat the key sequence to recall successively older commands.																			
Ctrl-N or Down Arrow ¹	Returns to more recent commands in the history buffer after recalling commands with Ctrl-P or the Up Arrow. Repeat the key sequence to recall successively more recent commands.																			
Cisco IOS 15.1 Effective date of registration: 11/28/2014	<table><tr><td>Left Arrow¹ or Ctrl-B</td><td>Back character</td><td>Moves the cursor one character to the left. When you enter a command that extends beyond a single line, you can press the Left Arrow or Ctrl-B keys repeatedly to scroll back toward the system prompt and verify the beginning of the command entry.</td></tr><tr><td>Right Arrow¹ or Ctrl-F</td><td>Forward character</td><td>Moves the cursor one character to the right.</td></tr><tr><td>Esc, B</td><td>Back word</td><td>Moves the cursor back one word.</td></tr><tr><td>Esc, F</td><td>Forward word</td><td>Moves the cursor forward one word.</td></tr><tr><td>Ctrl-A</td><td>Beginning of line</td><td>Moves the cursor to the beginning of the line.</td></tr><tr><td>Ctrl-E</td><td>End of line</td><td>Moves the cursor to the end of the command line.</td></tr></table> <p>Cisco IOS Configuration Fundamentals Command Reference (2010), at CF-189.</p>	Left Arrow ¹ or Ctrl-B	Back character	Moves the cursor one character to the left. When you enter a command that extends beyond a single line, you can press the Left Arrow or Ctrl-B keys repeatedly to scroll back toward the system prompt and verify the beginning of the command entry.	Right Arrow ¹ or Ctrl-F	Forward character	Moves the cursor one character to the right.	Esc, B	Back word	Moves the cursor back one word.	Esc, F	Forward word	Moves the cursor forward one word.	Ctrl-A	Beginning of line	Moves the cursor to the beginning of the line.	Ctrl-E	End of line	Moves the cursor to the end of the command line.	<p>3.2.3 Cursor Movement Keystrokes</p> <p>EOS supports these cursor movement keystrokes:</p> <ul style="list-style-type: none">• Ctrl-B or the Left Arrow key: Moves the cursor back one character.• Ctrl-F or the Right Arrow key: Moves the cursor forward one character.• Ctrl-A: Moves the cursor to the beginning of the command line.• Ctrl-E: Moves the cursor to the end of the command line.• Esc-B: Moves the cursor back one word.• Esc-F: Moves the cursor forward one word. <p>Arista User Manual v. 4.13.6F (4/14/2014), at 102.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 92; Arista User Manual, v. 4.11.1 (1/11/13), at 62; Arista User Manual v. 4.10.3 (10/22/12), at 54; Arista User Manual v. 4.9.3.2 (5/3/12), at 50; Arista User Manual v. 4.8.2 (11/18/11), at 46; Arista User Manual v. 4.7.3 (7/18/11), at 44; Arista User Manual v. 4.6.0 (12/22/2010), at 38.</p>
Left Arrow ¹ or Ctrl-B	Back character	Moves the cursor one character to the left. When you enter a command that extends beyond a single line, you can press the Left Arrow or Ctrl-B keys repeatedly to scroll back toward the system prompt and verify the beginning of the command entry.																		
Right Arrow ¹ or Ctrl-F	Forward character	Moves the cursor one character to the right.																		
Esc, B	Back word	Moves the cursor back one word.																		
Esc, F	Forward word	Moves the cursor forward one word.																		
Ctrl-A	Beginning of line	Moves the cursor to the beginning of the line.																		
Ctrl-E	End of line	Moves the cursor to the end of the command line.																		

Copyright Registration Information	Cisco	Arista								
Cisco NX-OS 4.0 Effective Date of registration: 11/13/2014	<table><tr><th>Channel Mode</th><th>Description</th></tr><tr><td>passive</td><td>LACP mode that places a port into a passive negotiating state, in which the port responds to LACP packets that it receives but does not initiate LACP negotiation.</td></tr><tr><td>active</td><td>LACP mode that places a port into an active negotiating state, in which the port initiates negotiations with other ports by sending LACP packets.</td></tr><tr><td>on</td><td>All static port channels, that is, that are not running LACP, remain in this mode. If you attempt to change the channel mode to active or passive before enabling LACP, the device returns an error message. You enable LACP on each channel by configuring the interface in that channel for the channel mode as either active or passive. When an LACP attempts to negotiate with an interface in the on state, it does not receive any LACP packets and becomes an individual link with that interface; it does not join the LACP channel group. The default port-channel mode is on.</td></tr></table>	Channel Mode	Description	passive	LACP mode that places a port into a passive negotiating state, in which the port responds to LACP packets that it receives but does not initiate LACP negotiation.	active	LACP mode that places a port into an active negotiating state, in which the port initiates negotiations with other ports by sending LACP packets.	on	All static port channels, that is, that are not running LACP, remain in this mode. If you attempt to change the channel mode to active or passive before enabling LACP, the device returns an error message. You enable LACP on each channel by configuring the interface in that channel for the channel mode as either active or passive. When an LACP attempts to negotiate with an interface in the on state, it does not receive any LACP packets and becomes an individual link with that interface; it does not join the LACP channel group. The default port-channel mode is on.	<p>Parameters</p> <ul style="list-style-type: none"><i>number</i> specifies a channel group ID. Values range from 1 through 1000.<i>LACP_MODE</i> specifies the interface LACP mode. Values include:<ul style="list-style-type: none"><i>mode on</i> Configures interface as a static port channel, disabling LACP. The switch does not verify or negotiate port channel membership with other switches.<i>mode active</i> Enables LACP on the interface in active negotiating state. The port initiates negotiations with other ports by sending LACP packets.<i>mode passive</i> Enables LACP on the interface in a passive negotiating state. The port responds to LACP packets but cannot start LACP negotiations. <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 469.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 403; Arista User Manual, v. 4.11.1 (1/11/13), at 336; Arista User Manual v. 4.10.3 (10/22/12), at 294; Arista User Manual v. 4.9.3.2 (5/3/12), at 278; Arista User Manual v. 4.8.2 (11/18/11), at 210; Arista User Manual v. 4.7.3 (7/18/11), at 424; Arista User Manual v. 4.6.0 (12/22/2010), at 271.</p>
	Channel Mode	Description								
passive	LACP mode that places a port into a passive negotiating state, in which the port responds to LACP packets that it receives but does not initiate LACP negotiation.									
active	LACP mode that places a port into an active negotiating state, in which the port initiates negotiations with other ports by sending LACP packets.									
on	All static port channels, that is, that are not running LACP, remain in this mode. If you attempt to change the channel mode to active or passive before enabling LACP, the device returns an error message. You enable LACP on each channel by configuring the interface in that channel for the channel mode as either active or passive. When an LACP attempts to negotiate with an interface in the on state, it does not receive any LACP packets and becomes an individual link with that interface; it does not join the LACP channel group. The default port-channel mode is on.									
Cisco NX-OS 4.0 Effective Date of registration: 11/13/2014	<p>encapsulation dot1Q</p> <p>To enable IEEE 802.1Q encapsulation of traffic on a specified subinterface in a virtual LAN (VLAN), use the encapsulation dot1q command in subinterface configuration mode. To disable encapsulation, use the no form of this command.</p> <p>encapsulation dot1Q <i>vlan-id</i></p> <p>no encapsulation dot1Q <i>vlan-id</i></p> <p>Cisco NX-OS Interfaces Command Reference (2008), Release 4.0, at IF-8.</p>	<p>encapsulation dot1q vlan</p> <p>The encapsulation dot1q vlan command enables Layer 2 802.1Q encapsulation of traffic on a specified subinterface in a VLAN. The default VLAN for all interfaces is VLAN 1.</p> <p>The no encapsulation dot1q vlan and default encapsulation dot1q vlan commands restore the default VLAN to the configuration mode interface by removing the corresponding encapsulation dot1q vlan command from running-config.</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 774.</p>								

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 4.0</p> <p>Effective Date of registration: 11/13/2014</p>	<p>switchport trunk native vlan</p> <p>To change the native VLAN ID when the interface is in trunking mode, use the switchport trunk native vlan command. To return the native VLAN ID to VLAN 1, use the no form of this command.</p> <p>switchport trunk native vlan <i>vlan-id</i></p> <p>no switchport trunk native vlan</p> <p>Cisco NX-OS Interfaces Command Reference (2008), Release 4.0, at IF-35.</p>	<p>switchport trunk native vlan</p> <p>The switchport trunk native vlan command specifies the trunk mode native VLAN for the configuration mode interface. Interfaces in trunk mode associate untagged frames with the native VLAN. Trunk mode interfaces can also be configured to drop untagged frames. The default native VLAN for all interfaces is VLAN 1.</p> <p>The no switchport trunk native vlan and default switchport trunk native vlan commands restore VLAN 1 as the trunk mode native VLAN to the configuration mode interface by removing the corresponding switchport trunk native vlan command from <i>running-config</i>.</p> <p>Platform all Command Mode <i>Interface Ethernet Configuration</i> <i>Interface Port-channel Configuration</i></p> <p>Command Syntax</p> <p>switchport trunk native vlan <i>VLAN_ID</i></p> <p>no switchport trunk native vlan</p> <p>default switchport trunk native vlan</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 800.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 647; Arista User Manual, v. 4.11.1 (1/11/13), at 500; Arista User Manual v. 4.10.3 (10/22/12), at 418; Arista User Manual v. 4.9.3.2 (5/3/12), at 357.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 4.0</p> <p>Effective Date of registration: 11/13/2014</p>	<p>— Rapid per VLAN Spanning Tree Plus (Rapid PVST+) and Multiple Spanning Tree (MST) have built-in compatibility mechanisms that allow them to interact properly with other versions of IEEE spanning tree or other regions. For example, a bridge running Rapid PVST+ can send 802.1D bridge protocol data units (BPDUs) on one of its ports when it is connected to a legacy bridge. An MST bridge can detect that a port is at the boundary of a region when it receives a legacy BPDU or an MST BPDU that is associated with a different region.</p> <p>These mechanisms are not always able to revert to the most efficient mode. For example, a Rapid PVST+ bridge that is designated for a legacy 802.1D bridge stays in 802.1D mode even after the legacy bridge has been removed from the link. Similarly, an MST port assumes that it is a boundary port when the bridges to which it is connected have joined the same region.</p> <p>To force the MST port to renegotiate with the neighbors, enter the clear spanning-tree detected-protocol command.</p> <p>If you enter the clear spanning-tree detected-protocol command with no arguments, the command is applied to every port of the device.</p> <p>This command does not require a license.</p> <p>Cisco NX-OS Layer 2 Switching Command Reference (2008), Release 4.0, at L2-5.</p>	<p>20.2.1.4 Version Interoperability</p> <p>A network can contain switches running different spanning tree versions. The common spanning tree (CST) is a single forwarding path the switch calculates for STP, RSTP, MSTP, and Rapid-PVST topologies in networks containing multiple spanning tree variations.</p> <p>In multi-instance topologies, the following instances correspond to the CST:</p> <ul style="list-style-type: none"> • Rapid-PVST VLAN 1 • MST IST (instance 0) <p>RSTP and MSTP are compatible with other spanning tree versions:</p> <ul style="list-style-type: none"> • An RSTP bridge sends 802.1D (original STP) BPDUs on ports connected to an STP/bridge. • RSTP bridges operating in 802.1D mode remain in 802.1D mode even after all STP bridges are removed from their links. • An MST bridge can detect that a port is at a region boundary when it receives an STP BPDU or an MST BPDU from a different region. • MST ports assume they are boundary ports when the bridges to which they connect join the same region. <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 953.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 831; Arista User Manual, v. 4.11.1 (1/11/13), at 649; Arista User Manual v. 4.10.3 (10/22/12), at 563; Arista User Manual v. 4.9.3.2 (5/3/12), at 483; Arista User Manual v. 4.8.2 (11/18/11), at 357; Arista User Manual v. 4.7.3 (7/18/11), at 231.</p>
<p>Cisco NX-OS 4.0</p> <p>Effective Date of registration: 11/13/2014</p>	<p>When you enable this BPDU Guard command globally, the command applies only to spanning tree edge ports. See spanning-tree port type edge bpduguard default for more information on the global command for BPDU Guard. However, when you enable this feature on an <i>interface</i>, it applies to that interface <i>regardless</i> of the spanning tree port type.</p> <p>This command has three states:</p> <ul style="list-style-type: none"> • spanning-tree bpduguard enable—Unconditionally enables BPDU Guard on the interface. • spanning-tree bpduguard disable—Unconditionally disables BPDU Guard on the interface. • no spanning-tree bpduguard—Enables BPDU Guard on the interface if it is an operational spanning tree edge port and if the spanning-tree port type edge bpduguard default command is configured. <p>Cisco NX-OS Layer 2 Switching Command Reference (2008), Release 4.0, at L2-31.</p>	<p>The spanning-tree bpduguard interface configuration command controls BPDU guard on the configuration mode interface. This command takes precedence over the default setting configured by spanning-tree portfast bpduguard default.</p> <ul style="list-style-type: none"> • spanning-tree bpduguard enable enables BPDU guard on the interface. • spanning-tree bpduguard disable disables BPDU guard on the interface. • no spanning-tree bpduguard reverts the interface to the default BPDU guard setting. <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 968.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 847; Arista User Manual, v. 4.11.1 (1/11/13), at 665; Arista User Manual v. 4.10.3 (10/22/12), at 579; Arista User Manual v. 4.9.3.2 (5/3/12), at 498; Arista User Manual v. 4.8.2 (11/18/11), at 372; Arista User Manual v. 4.7.3 (7/18/11), at 246.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 4.0</p> <p>Effective Date of registration: 11/13/2014</p>	<p>Understanding Loop Guard</p> <p>Loop Guard helps prevent bridging loops that could occur because of a unidirectional link failure on a point-to-point link.</p> <p>Cisco NX-OS Layer 2 Switching Configuration Guide (2008), Release 4.0, at 7-6.</p>	<p>20.3.3 Port Roles and Rapid Convergence</p> <p>Spanning Tree provides the following options for controlling port configuration and operation:</p> <ul style="list-style-type: none"> • PortFast: Allows ports to skip the listening and learning states before entering forwarding state. • Port Type and Link Type: Designates ports for rapid transitions to the forwarding state. • Root Guard: Prevents a port from becoming root port or blocked port. • Loop Guard: Prevents loops resulting from a unidirectional link failure on a point-to-point link. • Bridge Assurance: Prevents loops caused by unidirectional links or a malfunctioning switch. <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 964.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 842; Arista User Manual, v. 4.11.1 (1/11/13), at 660; Arista User Manual v. 4.10.3 (10/22/12), at 574; Arista User Manual v. 4.9.3.2 (5/3/12), at 494; Arista User Manual v. 4.8.2 (11/18/11), at 368; Arista User Manual v. 4.7.3 (7/18/11), at 242.</p>
<p>Cisco NX-OS 4.0</p> <p>Effective Date of registration: 11/13/2014</p>	<p>Bridge Assurance is enabled by default and can only be disabled globally. Also, Bridge Assurance can be enabled only on spanning tree network ports that are point-to-point links. Finally, both ends of the link must have Bridge Assurance enabled. If the device on one side of the link has Bridge Assurance enabled and the device on the other side either does not support Bridge Assurance or does not have this feature enabled, the connecting port is blocked.</p> <p>Cisco NX-OS Layer 2 Switching Configuration Guide (2008), Release 4.0, at 7-3.</p>	<p>spanning-tree bridge assurance</p> <p>The spanning-tree bridge assurance command enables bridge assurance on all ports with a port type of <i>network</i>. Bridge assurance protects against unidirectional link failure, other software failure, and devices that quit running a spanning tree algorithm.</p> <p>Bridge assurance is available only on spanning tree <i>network</i> ports on point-to-point links. Both ends of the link must have bridge assurance enabled. If the device on one side of the link has bridge assurance enabled and the device on the other side either does not support bridge assurance or does not have it enabled, the bridge assurance enabled port is blocked.</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1002.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 880; Arista User Manual, v. 4.11.1 (1/11/13), at 698; Arista User Manual v. 4.10.3 (10/22/12), at 612; Arista User Manual v. 4.9.3.2 (5/3/12), at 531; Arista User Manual v. 4.8.2 (11/18/11), at 403; Arista User Manual v. 4.7.3 (7/18/11), at 252.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 4.0</p> <p>Effective Date of registration: 11/13/2014</p>	<p>A regular expression is entered as part of a command and is a pattern made up of symbols, letters, and numbers that represent an input string for matching (or sometimes not matching). Matching the string to the specified pattern is called pattern matching.</p> <p>Cisco NX-OS Unicast Routing Command Reference (2008), Release 4.0, at A-1.</p>	<p>3.2.6 Regular Expressions</p> <p>A regular expression is pattern of symbols, letters, and numbers that represent an input string for matching an input string entered as a CLI parameter. The switch uses regular expression pattern matching in several BGP commands.</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 106.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 94; Arista User Manual, v. 4.11.1 (1/11/13), at 64; Arista User Manual v. 4.10.3 (10/22/12), at 56; Arista User Manual v. 4.9.3.2 (5/3/12), at 52; Arista User Manual v. 4.8.2 (11/18/11), at 48.</p>

Copyright Registration Information	Cisco		Arista
Cisco NX-OS 4.0 Effective Date of registration: 11/13/2014	\$	Matches the character or null string at the end of an input string.	123\$ matches 0123, but not 1234
	*	Matches zero or more sequences of the character preceding the asterisk. Also acts as a wildcard for matching any number of characters.	5* matches any occurrence of the number 5 including none
	+	Matches one or more sequences of the character preceding the plus sign.	8+ requires there to be at least one number 8 in the string to be match
	() []	Nest characters for matching. Separate endpoints of a range with a dash (-).	(17)* matches any number of the two-character string 17
		Concatenates constructs. Matches one of the characters or character patterns on either side of the vertical bar.	A(B C)D matches ABD and ACD, not AD, ABCD, ABB, or ACCD
	-	Replaces a long regular expression list by matching a comma (,), left brace ({}), right brace (}), the beginning of the input string, the end of the input string, or a space.	The characters _1300_ can match of the following strings: <ul style="list-style-type: none">• ^1300\$• ^1300space• space1300• {1300,• ,1300,• {1300}• ,1300,

Copyright Registration Information	Cisco	Arista						
Cisco NX-OS 4.0 Effective Date of registration: 11/13/2014	<p>The order for matching using the * or + character is longest construct first. Nested constructs are matched from the outside in. Concatenated constructs are matched beginning at the left side. If a regular expression can match two different parts of an input string, it will match the earliest part first.</p> <p>Cisco NX-OS Unicast Routing Command Reference (2008), Release 4.0, at A-3.</p>	<p>The order for matching using the * or + character is longest construct first. Nested constructs are matched from the outside in. Concatenated constructs are matched beginning at the left side. If a regular expression can match two different parts of an input string, it matches the earliest part first.</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 107.</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 105; Arista User Manual v. 4.12.3 (7/17/13), at 95; Arista User Manual, v. 4.11.1 (1/11/13), at 65; Arista User Manual v. 4.10.3 (10/22/12), at 57; Arista User Manual v. 4.9.3.2 (5/3/12), at 53; Arista User Manual v. 4.8.2 (11/18/11), at 49.</p>						
Cisco NX-OS 4.0 Effective Date of registration: 11/13/2014	<p>max-metric router-lsa (OSPF)</p> <p>To configure the Open Shortest Path First (OSPF) protocol to advertise a maximum metric so that other routers do not prefer the router as an intermediate hop in their shortest path first (SPF) calculations, use the max-metric router-lsa command. To disable the advertisement of a maximum metric, use the no form of this command.</p> <p>max-metric router-lsa [on-startup [seconds] wait-for bgp tag]]</p> <p>no max-metric router-lsa [on-startup [seconds] wait-for bgp tag]]</p> <p>Cisco NX-OS Unicast Routing Command Reference (2008), Release 4.0, at L3-272.</p>	<p>max-metric router-lsa (OSPFv2)</p> <p>The max-metric router-lsa command allows the OSPF protocol to advertise a maximum metric so that other routers do not prefer the router as an intermediate hop in their SPF calculations.</p> <p>The no max-metric router-lsa and default max-metric router-lsa commands disable the advertisement of a maximum metric.</p> <table><tr><td>Platform</td><td>all</td></tr><tr><td>Command Mode</td><td>Router-OSPF Configuration</td></tr></table> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1439.</p>	Platform	all	Command Mode	Router-OSPF Configuration		
Platform	all							
Command Mode	Router-OSPF Configuration							
Cisco NX-OS 4.0 Effective Date of registration: 11/13/2014	<table><tr><th>Syntax</th><th>Description</th></tr><tr><td>on-startup seconds</td><td>(Optional) Configures the router to advertise a maximum metric at startup. (Optional) Maximum metric (in seconds) that is advertised for the specified time interval. The configurable range is from 5 to 86400 seconds. The default is 600 seconds.</td></tr><tr><td>wait-for bgp tag</td><td>(Optional) Advertises a maximum metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired. The default timer is 600 seconds.</td></tr></table> <p>Cisco NX-OS Unicast Routing Command Reference (2008), Release 4.0, at L3-272.</p>	Syntax	Description	on-startup seconds	(Optional) Configures the router to advertise a maximum metric at startup. (Optional) Maximum metric (in seconds) that is advertised for the specified time interval. The configurable range is from 5 to 86400 seconds. The default is 600 seconds.	wait-for bgp tag	(Optional) Advertises a maximum metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired. The default timer is 600 seconds.	<p>on-startup wait-for-bgp Configures the router to advertise a maximum metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired. The default timer is 600 seconds.</p> <p>on-startup <5 to 86400> Sets the maximum metric temporarily after a reboot to originate router LSAs with the max-metric value.</p> <p>wait-for-bgp or an on-start time value is not included in no and default commands.</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1439.</p>
Syntax	Description							
on-startup seconds	(Optional) Configures the router to advertise a maximum metric at startup. (Optional) Maximum metric (in seconds) that is advertised for the specified time interval. The configurable range is from 5 to 86400 seconds. The default is 600 seconds.							
wait-for bgp tag	(Optional) Advertises a maximum metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired. The default timer is 600 seconds.							

Copyright Registration Information	Cisco	Arista						
Cisco NX-OS 4.0 Effective Date of registration: 11/13/2014	<p>The <code>cluster-id</code> command is used to assign a cluster ID to a route reflector when the cluster has one or more route reflectors. Multiple route reflectors are deployed in a cluster to increase redundancy and avoid a single point of failure. <u>When multiple route reflectors are configured in a cluster, the same cluster ID is assigned to all route reflectors. This allows all route reflectors in the cluster to recognize updates from peers in the same cluster and reduces the number of updates that need to be stored in BGP routing tables.</u></p> <p>Cisco NX-OS Unicast Routing Command Reference (2008), Release 4.0, at L3-564.</p>	<p>When using route reflectors, an AS is divided into clusters. A cluster consists of one or more route reflectors and a group of clients to which they re-advertise route information. <u>Multiple route reflectors can be configured in the same cluster</u> to increase redundancy and avoid a single point of failure. Each route reflector has a cluster ID. If the cluster has a single route reflector, the cluster ID is its router ID. If a cluster has multiple route reflectors, a 4-byte cluster ID is assigned to all route reflectors in the cluster. All of them must be configured with the same cluster ID so that they can recognize updates from other route reflectors in the same cluster. The <code>bgp cluster-id</code> command configures the cluster ID in a cluster with multiple route reflectors.</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1549.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1331; Arista User Manual, v. 4.11.1 (1/11/13), at 1081; Arista User Manual v. 4.10.3 (10/22/12), at 893; Arista User Manual v. 4.9.3.2 (5/3/12), at 665.</p>						
Cisco NX-OS 4.0 Effective Date of registration: 11/13/2014	<p>timers basic</p> <p>To adjust the Routing Information Protocol (RIP) network timers, use the <code>timers basic</code> command in router address-family configuration mode. To restore the default timers, use the <code>no</code> form of this command.</p> <p><code>timers basic update invalid holddown flush</code></p> <p><code>no timers basic</code></p> <table><tr><th>Syntax</th><th>Description</th></tr><tr><td><code>update</code></td><td>Rate (in seconds) at which updates are sent. The default is 30 seconds.</td></tr><tr><td><code>invalid</code></td><td>Interval of time (in seconds) after which a route is declared invalid; it should be at least three times the value of the <code>update</code> argument. A route becomes invalid when no updates refresh the route. <u>The route then enters into a <code>holddown</code> state where it is marked as inaccessible and advertised as unreachable. However, the route is still used to forward packets. The default is 180 seconds.</u></td></tr></table> <p>Cisco NX-OS Unicast Routing Command Reference (2008), Release 4.0, at L3-538.</p>	Syntax	Description	<code>update</code>	Rate (in seconds) at which updates are sent. The default is 30 seconds.	<code>invalid</code>	Interval of time (in seconds) after which a route is declared invalid; it should be at least three times the value of the <code>update</code> argument. A route becomes invalid when no updates refresh the route. <u>The route then enters into a <code>holddown</code> state where it is marked as inaccessible and advertised as unreachable. However, the route is still used to forward packets. The default is 180 seconds.</u>	<p>timers basic (RIP)</p> <p>The <code>timers basic</code> command configures the update interval, the expiration time, and the deletion time for routes received and sent through RIP. The command requires value declaration of all values.</p> <ul style="list-style-type: none">The update time is the interval between unsolicited route responses. The default is 30 seconds.The expiration time is initialized when a route is established and any time an update is received for the route. <u>If the specified period elapses from the last time the route update was received, then the route is marked as inaccessible and advertised as unreachable. However, the route forwards packets until the deletion time expires. The default value is 180 seconds.</u> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1671.</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 1621; Arista User Manual v. 4.12.3 (7/17/13), at 1433; Arista User Manual, v. 4.11.1 (1/11/13), at 1179; Arista User Manual v. 4.10.3 (10/22/12), at 989; Arista User Manual v. 4.9.3.2 (5/3/12), at 748; Arista User Manual v. 4.8.2 (11/18/11), at 570.</p>
Syntax	Description							
<code>update</code>	Rate (in seconds) at which updates are sent. The default is 30 seconds.							
<code>invalid</code>	Interval of time (in seconds) after which a route is declared invalid; it should be at least three times the value of the <code>update</code> argument. A route becomes invalid when no updates refresh the route. <u>The route then enters into a <code>holddown</code> state where it is marked as inaccessible and advertised as unreachable. However, the route is still used to forward packets. The default is 180 seconds.</u>							

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 4.0</p> <p>Effective Date of registration: 11/13/2014</p>	<p>isis hello-multiplier</p> <p>To specify the number of Intermediate System-to-Intermediate System (IS-IS) hello packets a neighbor must miss before the router should declare the adjacency as down, use the isis hello-multiplier command in interface configuration mode. To restore the default value, use the no form of this command.</p> <p>isis hello-multiplier <i>multiplier</i> {level-1 level-2}</p> <p>no isis hello-multiplier {level-1 level-2}</p> <p>Cisco NX-OS Unicast Routing Command Reference (2008), Release 4.0, at L3-224.</p>	<p>isis hello-multiplier</p> <p>The isis hello-multiplier command specifies the number of IS-IS hello packets a neighbor must miss before the device should declare the adjacency as down.</p> <p>Each hello packet contains a hold time. The hold time informs the receiving devices how long to wait without seeing another hello from the sending device before considering the sending device down. The isis hello-multiplier command is used to calculate the hold time announced in hello packets by multiplying this number with the configured isis hello-interval.</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1685.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1447.</p>
<p>Cisco NX-OS 4.0</p> <p>Effective Date of registration: 11/13/2014</p>	<p>Local Proxy ARP</p> <p>You can use local Proxy ARP to enable a device to respond to ARP requests for IP addresses within a subnet where normally no routing is required. When you enable local Proxy ARP, ARP responds to all ARP requests for IP addresses within the subnet and forwards all traffic between hosts in the subnet. Use this feature only on subnets where hosts are intentionally prevented from communicating directly by the configuration on the device to which they are connected.</p> <p>Cisco NX-OS Unicast Routing Configuration Guide (2008), Release 4.0, at 2-5.</p>	<p>ip local-proxy-arp</p> <p>The ip local-proxy-arp command enables local proxy ARP (Address Resolution Protocol) on the configuration mode interface. Local proxy ARP programs the switch to respond to ARP requests for IP addresses within a subnet where routing is not normally required. A typical local proxy arp application is supporting isolated private VLANs that communicate with each other by routing packets.</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1276.</p> <p><i>See also</i> Arista User Manual v. 4.13.6F (4/14/2014), at 1231; Arista User Manual v. 4.12.3 (7/17/13), at 1073; Arista User Manual, v. 4.11.1 (1/11/13), at 856; Arista User Manual v. 4.10.3 (10/22/12), at 707.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 4.0</p> <p>Effective Date of registration: 11/13/2014</p>	<p>IS-IS Overview</p> <p>IS-IS sends a <i>hello packet</i> out every configured interface to discover IS-IS neighbor routers. The hello packet contains information, such as the authentication, area, and supported protocols, which the receiving interface uses to determine compatibility with the originating interface. Compatible interfaces form adjacencies, which update routing information in the link-state database through link-state update messages (LSFs). By default, the router sends a periodic LSP refresh every 10 minutes and the LSPs remain in the link-state database for 20 minutes (the LSP lifetime). If the router does not receive an LSP refresh before the end of the LSP lifetime, the router deletes the LSP from the database. The LSP interval must be less than the LSP lifetime or the LSPs time out before they are refreshed.</p> <p>IS-IS Areas</p> <p>You can design IS-IS networks as a single area that includes all routers in the network or as multiple areas that connect into a backbone or Level 2 area. Routers in a nonbackbone area are Level 1 routers which establish adjacencies within a local area (intra-area routing). Level 2 area routers establish adjacencies to other Level 2 routers and perform routing between Level 1 areas (inter-area routing). A router can have both Level 1 and Level 2 areas configured. These Level 1/Level 2 routers act as area border routers which route information from the local area to the Level 2 backbone area (see Figure 8-1).</p> <p>Within a Level 1 area, routers know how to reach all other routers in that area. Between areas, routers know how to reach the area border router to get to the Level 2 area. The Level 2 routers know how to reach other area border routers and other Level 2 routers. Level 1/Level 2 routers straddle the boundary between two areas, routing traffic to and from the Level 2 backbone area.</p> <p>Each IS-IS instance in Cisco NX-OS supports either a single Level 1 or Level 2 area, or one of each. By default, all IS-IS instances automatically support Level 1 and Level 2 routing.</p> <p>Cisco NX-OS Unicast Routing Configuration Guide, Release 4.0, at 8-2.</p>	<p>29.2 IS-IS Description</p> <p>IS-IS sends a hello packet out every configured interface to discover IS-IS neighbor routers. The hello packet contains information, which the receiving interface uses to determine compatibility with the originating interface. Compatible interfaces form adjacencies, which update routing information in the link-state database through link-state update messages (LSFs). If the router does not receive an LSP refresh before the end of the LSP lifetime, the device deletes the LSP from the database.</p> <p>Terms of IS-IS Routing Protocol</p> <p>The following terms are used when configuring IS-IS.</p> <ul style="list-style-type: none"> • NET and System ID – Each IS-IS instance has an associated network entity title (NET). The NET consists of the IS-IS system ID, which uniquely identifies the IS-IS instance in the area and the area ID. • Designated Intermediate System – IS-IS uses a Designated Intermediate System (DIS) in broadcast networks to prevent each device from forming unnecessary links with every other device on the broadcast network. IS-IS devices send LSPs to the DIS, which manages all the link-state information for the broadcast network. You can configure the IS-IS priority that IS-IS uses to select the DIS in an area. • IS-IS Areas – You can design IS-IS networks as a single area that includes all routers in the network or as multiple areas that connect into a backbone or Level 2 area. Routers in a nonbackbone area are Level 1 routers that establish adjacencies within a local area (intra-area routing). Level 2 area routers establish adjacencies to other Level 2 routers and perform routing between Level 1 areas (inter-area routing). A router can have both Level 1 and Level 2 areas configured. • IS-IS Instances – Arista supports only one instance of the IS-IS protocol that run on the same node. • LSP – Link state packet (LSP) can switch link state information. LSPs fall into two types: Level 1 LSPs and Level 2 LSPs. Level 2 devices transmit Level 2 LSPs; Level-1 devices transmit Level 1 LSPs; Level 1-2 devices transmit both Level 2 LSPs and Level 1 LSPs. • Hello packets – Hello packets, can establish and maintain neighbor relationships. • Overload Bit – IS-IS uses the overload bit to tell other devices not to use the local router to forward traffic but to continue routing traffic destined for that local router. Possible conditions for setting the overload bit the device is in a critical condition. <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1674.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1436.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 4.0</p> <p>Effective Date of registration: 11/13/2014</p>	<p>PIM Register Messages</p> <p>PIM register messages are unicast to the RP by designated routers (DRs) that are directly connected to multicast sources. The PIM register message has the following functions:</p> <ul style="list-style-type: none"> To notify the RP that a source is actively sending to a multicast group. To deliver multicast packets sent by the source to the RP for delivery down the shared tree. <p>The DR continues to send PIM register messages to the RP until it receives a Register-Stop message from the RP. The RP sends a Register-Stop message in either of the following cases:</p> <ul style="list-style-type: none"> The RP has no receivers for the multicast group being transmitted. The RP has joined the SPT to the source but has not started receiving traffic from the source. <p>Cisco NX-OS Multicast Routing Configuration Guide (2008), Release 4.0, at 3-7.</p>	<p>Anycast-RP</p> <p>PIM Anycast-RP defines a single RP address that is configured on multiple routers. An anycast-RP set consists of the routers configured with the same anycast-RP address. Anycast-RP provides redundancy, protection and load balancing. The anycast-RP set supports all multicast groups.</p> <p>PIM register messages are sent to the RP by designated routers (DRs) that are directly connected to multicast sources. The DRs deliver these messages and can prime messages on the anycast-RP set members specified in the anycast-RP command. In a typical configuration, one command is required for each member of the anycast-RP set.</p> <p>The PIM register message has the following functions:</p> <ul style="list-style-type: none"> Notify the RP that a source is actively sending to a multicast group. Deliver multicast packets sent by the source to the RP for delivery down the shared tree. <p>The DR continues sending PIM register messages to the RP until it receives a Register-Stop message from the RP. The RP sends a Register-Stop message in either of the following cases:</p> <ul style="list-style-type: none"> The RP has no receivers for the multicast group being transmitted. The RP has joined the SPT to the source but has not started receiving traffic from the source. <p>The <code>ip pim anycast-rp</code> command configures the switch as a member of an anycast-RP set and establishes a communication link with another member of the set.</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1874.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1580; Arista User Manual, v. 4.11.1 (1/11/13), at 1274; Arista User Manual v. 4.10.3 (10/22/12), at 1005-06; Arista User Manual v. 4.9.3.2 (5/3/12), at 763-65; Arista User Manual v. 4.8.2 (11/18/11), at 639; Arista User Manual v. 4.7.3 (7/18/11), at 514.</p>
<p>Cisco NX-OS 4.0</p> <p>Effective Date of registration: 11/13/2014</p>	<p>If the supplicant is successfully authenticated (receives an Accept frame from the authentication server), the port state changes to authorized, and all frames from the authenticated supplicant are allowed through the port. If the authentication fails, the port remains in the unauthorized state, but authentication can be retried. If the authentication server cannot be reached, the authenticator can retransmit the request. If no response is received from the server after the specified number of attempts, authentication fails, and the supplicant is not granted network access.</p> <p>Cisco DCNM Security Configuration Guide (2008), Release 4.0, at 6-5.</p>	<p>11.3.3 Designating Authenticator Ports</p> <p>You have to designate ports as authenticator ports before you can configure their settings. There are three <code>dot1x port-control</code> commands for designating authenticator ports. The command you use is determined by whether or not the switch is part of an active network.</p> <p>If the switch is not part of an active network or is not forwarding traffic, you can use the <code>dot1x port-control auto</code> command to designate the authenticator ports. This command designates ports such that they immediately begin to function as authenticator ports, blocking all traffic until supplicants log on to the RADIUS server.</p> <p>If the client is successfully authenticated, the port state changes to authorized, and all frames from the authenticated client are allowed through the port. If the authentication fails, the port remains in the unauthorized state, but authentication can be retried. If the authentication server cannot be reached, the switch can retransmit the request. If no response is received from the server after the specified number of attempts, authentication fails, and network access is not granted.</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 558.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 4.0</p> <p>Effective Date of registration: 11/13/2014</p>	<p>Changing Global 802.1X Authentication Timers</p> <p>The following global 802.1X authentication timers are supported on the device:</p> <ul style="list-style-type: none"> Quiet-period timer—When the device cannot authenticate the supplicant, the device remains idle for a set period of time, and then tries again. The quiet-period timer value determines the idle period. An authentication failure might occur because the supplicant provided an invalid password. You can provide a faster response time to the user by entering a number smaller than the default. The default is 60 seconds. The range is from 1 to 65535. <p>Cisco DCNM Security Configuration Guide (2008), Release 4.0, at 6-14.</p>	<p>dot1x timeout quiet-period</p> <p>The <code>dot1x timeout quiet-period</code> command sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client. The range is 1 to 65535 seconds; the default is 60.</p> <p>When the switch cannot authenticate the client, the switch remains idle for a set period of time and then tries again. You can provide a faster response time to the user by entering a number smaller than the default.</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 569.</p>
<p>Cisco NX-OS 4.0</p> <p>Effective Date of registration: 11/13/2014</p>	<p>Enabling Periodic Reauthentication for an Interface</p> <p>You can enable periodic 802.1X reauthentication on an interface and specify how often it occurs. If you do not specify a time period before enabling reauthentication, the number of seconds between reauthentication defaults to the global value.</p> <p>Cisco DCNM Security Configuration Guide (2008), Release 4.0, at 6-14</p>	<p>dot1x timeout reauth-period</p> <p>The <code>dot1x timeout reauth-period</code> command specifies the time interval for reauthentication of clients on an authenticator port. Re-authentication must be enabled on a authenticator port for the timer to work. If you do not specify a time period before enabling re-authentication, the number of seconds between re-authentication attempts is 3600.</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 570.</p>
<p>Cisco NX-OS 4.0</p> <p>Effective Date of registration: 11/13/2014</p>	<p>If the supplicant is successfully authenticated (receives an Accept frame from the authentication server), the port state changes to authorized, and all frames from the authenticated supplicant are allowed through the port. If the authentication fails, the port remains in the unauthorized state, but authentication can be retried. If the authentication server cannot be reached, the authenticator can retransmit the request. If no response is received from the server after the specified number of attempts, authentication fails, and the supplicant is not granted network access.</p> <p>Cisco NX-OS Security Configuration Guide (2008), Release 4.0, at 7-5.</p>	<p>11.3.3 Designating Authenticator Ports</p> <p>You have to designate ports as authenticator ports before you can configure their settings. There are three <code>dot1x port-control</code> commands for designating authenticator ports. The command you use is determined by whether or not the switch is part of an active network.</p> <p>If the switch is not part of an active network or is not forwarding traffic, you can use the <code>dot1x port-control auto</code> command to designate the authenticator ports. This command designates ports such that they immediately begin to function as authenticator ports, blocking all traffic until supplicants log on to the RADIUS server.</p> <p>If the client is successfully authenticated, the port state changes to authorized, and all frames from the authenticated client are allowed through the port. If the authentication fails, the port remains in the unauthorized state, but authentication can be retried. If the authentication server cannot be reached, the switch can retransmit the request. If no response is received from the server after the specified number of attempts, authentication fails, and network access is not granted.</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 558.</p>

Copyright Registration Information	Cisco	Arista				
Cisco NX-OS 4.0 Effective Date of registration: 11/13/2014	<p>Changing Global 802.1X Authentication Timers</p> <p>The following global 802.1X authentication timers are supported on the NX-OS device:</p> <ul style="list-style-type: none">• Quiet-period timer—When the NX-OS device cannot authenticate the supplicant, the NX-OS device remains idle for a set period of time, and then tries again. The quiet-period timer value determines the idle period. An authentication failure might occur because the supplicant provided an invalid password. You can provide a faster response time to the user by entering a number smaller than the default. The default is 60 seconds. The range is from 1 to 65535. <p>Cisco NX-OS Security Configuration Guide (2008), Release 4.0, at 7-18.</p>	<p>dot1x timeout quiet-period</p> <p>The dot1x timeout quiet-period command sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client. The range is 1 to 65535 seconds; the default is 60.</p> <p>When the switch cannot authenticate the client, the switch remains idle for a set period of time and then tries again. You can provide a faster response time to the user by entering a number smaller than the default.</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 569.</p>				
Cisco NX-OS 4.0 Effective Date of registration: 11/13/2014	<p>aaa group server radius</p> <p>To create a RADIUS server group and enter RADIUS server group configuration mode, use the aaa group server radius command. To delete a RADIUS server group, use the no form of this command:</p> <pre>aaa group server radius group-name no aaa group server radius group-name</pre> <p>Cisco NX-OS Security Command Reference (2008), Release 4.0, at 17.</p>	<p>aaa group server radius</p> <p>The aaa group server radius command enters the server-group-radius configuration mode for the specified group name. The command creates the specified group if it was not previously created. Commands are available to add servers to the group.</p> <p>A server group is a collection of servers that are associated with a single label. Subsequent authorization and authentication commands access all servers in a group by invoking the group name. Server group members must be previously configured with a radius-server host command.</p> <p>The no aaa group server radius and default aaa group server radius commands delete the specified server group from <i>running-config</i>.</p> <table><tr><td>Platform</td><td>all</td></tr><tr><td>Command Mode</td><td>Global Configuration</td></tr></table> <p>Command Syntax</p> <pre>aaa group server radius group_name no aaa group server radius group_name default aaa group server radius group_name</pre> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 224.</p> <p><i>See also</i> Arista User Manual v. 4.13.6F (4/14/2014), at 217; Arista User Manual, v. 4.11.1 (1/11/13), at 126; Arista User Manual v. 4.12.3 (7/17/13), at 168; Arista User Manual v. 4.10.3 (10/22/12), at 118.</p>	Platform	all	Command Mode	Global Configuration
Platform	all					
Command Mode	Global Configuration					

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 4.0</p> <p>Effective Date of registration: 11/13/2014</p>	<p>Usage Guidelines The 802.1X quiet-period timeout is the number of seconds that the switch remains in the quiet state following a failed authentication exchange with a supplicant.</p> <p>You must use the feature <code>dot1x</code> command before you configure 802.1X.</p> <p>Cisco NX-OS Security Command Reference (2008), Release 4.0, at 119.</p>	<p>dot1x timeout quiet-period</p> <p>The <code>dot1x timeout quiet-period</code> command sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client. The range is 1 to 65535 seconds; the default is 00.</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 569.</p>
<p>Cisco NX-OS 4.0</p> <p>Effective Date of registration: 11/13/2014</p>	<p>ip dhcp snooping information option</p> <p>To enable the insertion and removal of option-82 information for DHCP packets, use the <code>ip dhcp snooping information option</code> command. To disable the insertion and removal of option-82 information, use the <code>no</code> form of this command.</p> <p><code>ip dhcp snooping information option</code> <code>no ip dhcp snooping information option</code></p> <p>Cisco NX-OS Security Command Reference (2008), Release 4.0, at 196.</p>	<p>Command Syntax</p> <p><code>ip dhcp snooping information option</code> <code>no ip dhcp snooping information option</code></p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1270.</p>
<p>Cisco NX-OS 4.0</p> <p>Effective Date of registration: 11/13/2014</p>	<p>SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the role in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet.</p> <p>Cisco NX-OS System Management Configuration Guide (2008), Release 4.0, at 7-2,</p>	<p>SNMPv3 is a security model which defines an authentication strategy that is configured for a user and the group in which the user resides. A security level is the permitted level of security within the model. A combination of a security model and a security level determines the security mechanism employed to handle an SNMP packet.</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1964.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1654; Arista User Manual, v. 4.11.1 (1/11/13), at 1342; Arista User Manual v. 4.10.3 (10/22/12), at 1108; Arista User Manual v. 4.9.3.2 (5/3/12), at 864; Arista User Manual v. 4.8.2 (11/18/11), at 675; Arista User Manual v. 4.7.3 (7/18/11), at 531.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 4.0</p> <p>Effective Date of registration: 11/13/2014</p>	<p>SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the role in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet.</p> <p>Cisco NX-OS System Management Configuration Guide (2010), Release 5.0, at 10-2.</p>	<p>SNMPv3 is a security model which defines an authentication strategy that is configured for a user and the group in which the user resides. A security level is the permitted level of security within the model. A combination of a security model and a security level determines the security mechanism employed to handle an SNMP packet.</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1964.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1654; Arista User Manual, v. 4.11.1 (1/11/13), at 1342; Arista User Manual v. 4.10.3 (10/22/12), at 1108; Arista User Manual v. 4.9.3.2 (5/3/12), at 864; Arista User Manual v. 4.8.2 (11/18/11), at 675; Arista User Manual v. 4.7.3 (7/18/11), at 531.</p>
<p>Cisco IOS XE 2.1</p> <p>Effective Date of registration: 11/24/2014</p>	<p>SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the role in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet.</p> <p>Configuring SNMP Support (2008), at 17.</p>	<p>SNMPv3 is a security model which defines an authentication strategy that is configured for a user and the group in which the user resides. A security level is the permitted level of security within the model. A combination of a security model and a security level determines the security mechanism employed to handle an SNMP packet.</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1964.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1654; Arista User Manual, v. 4.11.1 (1/11/13), at 1342; Arista User Manual v. 4.10.3 (10/22/12), at 1108; Arista User Manual v. 4.9.3.2 (5/3/12), at 864; Arista User Manual v. 4.8.2 (11/18/11), at 675; Arista User Manual v. 4.7.3 (7/18/11), at 531.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<p>snmp-server enable traps atm pvc</p> <p>...</p> <p>Usage Guidelines SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types. ATM notifications are defined in the CISCO-IETF-ATM2-PVCTRAP-MIB.mib file, available from the Cisco FTP site at http://www.cisco.com/public/mibs/v2/.</p> <p>Cisco IOS Asynchronous Transfer Mode Command Reference (2013), at 526.</p>	<p>snmp-server enable traps</p> <p>The snmp-server enable traps command enables the transmission of Simple Network Management Protocol (SNMP) notifications as traps or inform requests. This command enables both traps and inform requests for the specified notification types. The snmp-server host command specifies the notification type (traps or informs). Sending notifications requires at least one snmp-server host command.</p> <p>The snmp-server enable traps and no snmp-server enable traps commands, without an MIB parameter, specifies the default notification trap generation setting for all MIBs. These commands, when specifying an MIB, controls notification generation for the specified MIB. The default snmp-server enable traps command resets notification generation to the default setting for the specified MIB.</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1990.</p> <p><i>See also</i> Arista User Manual v. 4.13.6F (4/14/2014), at 1918; Arista User Manual v. 4.12.3 (7/17/13), at 1680; Arista User Manual, v. 4.11.1 (1/11/13), at 1365; Arista User Manual v. 4.10.3 (10/22/12), at 1132; Arista User Manual v. 4.9.3.2 (5/3/12), at 888; Arista User Manual v. 4.8.2 at 696; Arista User Manual v. 4.7.3 (7/18/11), at 552.</p>


Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<pre>Router# show interface cbr 6/0 CBR6/0 is up, line protocol is up Hardware is DCU MTU 0 bytes, BW 1544 Kbit, DLY 0 usec, rely 255/255, load 248/255 Encapsulation ET ATMCES_T1, loopback not set Last input 00:00:00, output 00:00:00, output hang never Last clearing of "show interface" counters never Queueing strategy: fifo Output queue 0/0, 0 drops; input queue 0/75, 0 drops 5 minute input rate 1507000 bits/sec, 3957 packets/sec 5 minute output rate 1507000 bits/sec, 3955 packets/sec 3025960 packets input, 142220120 bytes, 0 no buffer Received 0 broadcasts, 0 runts, 0 giants 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort 3030067 packets output, 142413149 bytes, 0 underruns 0 output errors, 0 collisions, 0 interface resets 0 output buffer failures, 0 output buffers swapped out</pre> <p>The table below describes the fields shown in the display.</p> <p>Cisco IOS Asynchronous Transfer Mode Command Reference (2013), at 460.</p>	<pre>switch#show interfaces ethernet 1 Ethernet1 is up, line protocol is up (connected) Hardware is Ethernet, address is 001c.7302.2fff (bia 001c.7302.2fff) MTU 9212 bytes, BW 10000000 Kbit Full-duplex, 10Gb/s, auto negotiation: off Last clearing of "show interface" counters never 5 minutes input rate 301 bps (0.0% with framing), 0 packets/sec 5 minutes output rate 0 bps (0.0% with framing), 0 packets/sec 2285370854005 packets input, 225028582832583 bytes Received 29769609741 broadcasts, 3073437605 multicast 113 runts, 1 giants 118 input errors, 117 CRC, 0 alignment, 18 symbol 27511409 PAUSE input 335031607678 packets output, 27845413138330 bytes Sent 14282316688 broadcasts, 54045824072 multicast 108 output errors, 0 collisions 0 late collision, 0 deferred 0 PAUSE output</pre> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 437.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 371; Arista User Manual, v. 4.11.1 (1/11/13), at 312; Arista User Manual v. 4.10.3 (10/22/12), at 270; Arista User Manual v. 4.9.3.2 (5/3/12), at 252.</p>

Copyright Registration Information	Cisco	Arista						
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<div><div>severity-level</div><div>(Optional) The number or name of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows (enter the number or the keyword): [0 emergencies] —System is unusable [1 alerts]—Immediate action needed [2 critical]—Critical conditions [3 errors]—Error conditions [4 warnings]—Warning conditions [5 notifications]—Normal but significant conditions [6 informational]—Informational messages [7 debugging]—Debugging messages</div></div> <div>Cisco IOS Cisco Networking Services Command Reference (2013), at 91.</div>	<div><div><div>• CONDITION Specifies condition level. Options include: — <no parameter> Specifies default condition level. — severity <condition-level> Name of the severity level at which messages should be logged</div><div>Valid condition-level options include: * 0 or emergencies System is unusable * 1 or alerts Immediate action needed * 2 or critical Critical conditions * 3 or errors Error conditions * 4 or warnings Warning conditions * 5 or notifications Normal but significant conditions * 6 or informational Informational messages * 7 or debugging Debugging messages</div></div><div>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 155.</div></div>						
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<table><tr><th>Command</th><th>Description</th></tr><tr><td>show debugging</td><td>Displays information about the types of debugging that are enabled.</td></tr><tr><td>show dot1x</td><td>Displays 802.1x statistics, administrative status, and operational status for the router or for the specified interface.</td></tr></table> <div>Cisco IOS Debug Command Reference – Commands A through D (2013), at 635.</div>	Command	Description	show debugging	Displays information about the types of debugging that are enabled.	show dot1x	Displays 802.1x statistics, administrative status, and operational status for the router or for the specified interface.	<div><div>show dot1x</div><div>The show dot1x command displays the 802.1x statistics, administrative status, and operational status for the specified interface.</div><div>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 572.</div></div>
Command	Description							
show debugging	Displays information about the types of debugging that are enabled.							
show dot1x	Displays 802.1x statistics, administrative status, and operational status for the router or for the specified interface.							

Copyright Registration Information	Cisco	Arista				
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<table><tr><th>Command</th><th>Description</th></tr><tr><td>show ip igmp interface</td><td>Displays multicast-related information about an interface.</td></tr></table> <p>Cisco IOS Debug Command Reference – Commands I through L (2013), at 297.</p>	Command	Description	show ip igmp interface	Displays multicast-related information about an interface.	<p>show ip igmp interface</p> <p>The show ip igmp interface command displays multicast-related information about an interface.</p> <ul style="list-style-type: none">show ip igmp interface – displays all multicast information for all interfacesshow ip igmp interface <i>int-name</i> – displays multicast information for the specified interfaces. <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1850.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1558; Arista User Manual, v. 4.11.1 (1/11/13), at 1253; Arista User Manual v. 4.10.3 (10/22/12), at 1038; Arista User Manual v. 4.9.3.2 (5/3/12), at 796; Arista User Manual v. 4.8.2 (11/18/11), at 614; Arista User Manual v. 4.7.3 (7/18/11), at 491; Arista User Manual v. 4.6.0 (12/22/2010), at 337.</p>
Command	Description					
show ip igmp interface	Displays multicast-related information about an interface.					
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<pre>Router# show interfaces Ethernet0/0 is up, line protocol is up Hardware is AmdP2, address is aabb.cc03.6c00 (bia aabb.cc03.6c00) Internet address is 172.17.1.1/16 MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, reliability 255/255, txload 1/255, rxload 1/255 Encapsulation ARPA, loopback not set Keepalive set (10 sec) ARP type: ARPA, ARP Timeout 04:00:00 Last input never, output 00:00:06, output hang never Last clearing of "show interface" counters never Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0 Queueing strategy: fifo Output queue: 0/40 (size/max) 5 minute input rate 0 bits/sec, 0 packets/sec 5 minute output rate 0 bits/sec, 0 packets/sec 0 packets input, 0 bytes, 0 no buffer Received 0 broadcasts, 0 runts, 0 giants, 0 throttles 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored 0 input packets with dribble condition detected 11 packets output, 1648 bytes, 0 underruns 0 output errors, 0 collisions, 1 interface resets 0 babbles, 0 late collision, 0 deferred 0 lost carrier, 0 no carrier 0 output buffer failures, 0 output buffers swapped out</pre> <p>Cisco Configuration Fundamentals Configuration Guide, Cisco IOS Release 15M&T (2013), at 44.</p>	<pre>switch#show interfaces ethernet 1 Ethernet1 is up, line protocol is up (connected) Hardware is Ethernet, address is 001c.7302.2fff (bia 001c.7302.2fff) MTU 9212 bytes, BW 10000000 Kbit Full-duplex, 10Gb/s, auto negotiation: off Last clearing of "show interface" counters never 5 minutes input rate 301 bps (0.0% with framing), 0 packets/sec 5 minutes output rate 0 bps (0.0% with framing), 0 packets/sec 2285370854005 packets input, 225028582832583 bytes Received 29769609741 broadcasts, 3073437605 multicast 113 runts, 1 giants 118 input errors, 117 CRC, 0 alignment, 18 symbol 27511409 PAUSE input 335031607678 packets output, 27845413138330 bytes Sent 14282316688 broadcasts, 54045824072 multicast 108 output errors, 0 collisions 0 late collision, 0 deferred 0 PAUSE output</pre> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 437.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 371; Arista User Manual, v. 4.11.1 (1/11/13), at 312; Arista User Manual v. 4.10.3 (10/22/12), at 270; Arista User Manual v. 4.9.3.2 (5/3/12), at 252.</p>				

Copyright Registration Information	Cisco	Arista								
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<p>Use the <code>show interface interface-type interface-number</code> command to display the information and statistics for Ethernet 0 on R4.</p> <pre>R4> show interface ethernet 0 Ethernet0 is up, line protocol is up Hardware is Lance, address is 00e0.1eb8.eb0e (bia 00e0.1eb8.eb0e) The MAC address for Ethernet 0 on R4 is 00e0 1eb8 eb0e. The format of the client identifier for this interface is nullcisco-00e0.1eb8.eb0e-ct0.</pre> <p>Cisco Configuration Fundamentals Configuration Guide, Cisco IOS Release 15M&T (2013), at 81.</p>	<p>This command assigns the MAC address of 001c.2804.17e1 to Ethernet interface 7, then displays interface parameters, including the assigned address.</p> <pre>switch(config)#interface ethernet 7 switch(config-if-Et7)#mac-address 001c.2804.17e1 switch(config-if-Et7)#show interface ethernet 7 Ethernet3 is up, line protocol is up (connected) Hardware is Ethernet, address is 001c.2804.17e1 (bia 001c.7312.02e2)</pre> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 437.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 371; Arista User Manual, v. 4.11.1 (1/11/13), at 312; Arista User Manual v. 4.10.3 (10/22/12), at 270; Arista User Manual v. 4.9.3.2 (5/3/12), at 252.</p>								
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<table><thead><tr><th>Command</th><th>Description</th></tr></thead><tbody><tr><td>show ip mfib</td><td>Displays the forwarding entries and interfaces in the IPv4 MFIB</td></tr><tr><td>show ip mfib active</td><td>Displays information from the IPv4 MFIB about the rate at which active multicast sources are sending to multicast groups.</td></tr><tr><td>show ip mfib count</td><td>Displays a summary of traffic statistics from the IPv4 MFIB about multicast sources and groups.</td></tr></tbody></table> <p>Cisco IOS Multicast Command Reference (2013), at 17.</p>	Command	Description	show ip mfib	Displays the forwarding entries and interfaces in the IPv4 MFIB	show ip mfib active	Displays information from the IPv4 MFIB about the rate at which active multicast sources are sending to multicast groups.	show ip mfib count	Displays a summary of traffic statistics from the IPv4 MFIB about multicast sources and groups.	<p>The <code>show ip mfib</code> command displays the forwarding entries and interfaces in the IPv4 MFIB</p> <ul style="list-style-type: none">• <code>show ip mfib</code> displays MFIB information for hardware forwarded routes.• <code>show ip mfib software</code> displays MFIB information for software forwarded routes. <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1755.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1484; Arista User Manual, v. 4.11.1 (1/11/13), at 1186; Arista User Manual v. 4.10.3 (10/22/12), at 1020; Arista User Manual v. 4.9.3.2 (5/3/12), at 778; Arista User Manual v. 4.8.2 (11/18/11), at 597; Arista User Manual v. 4.7.3 (7/18/11), at 477; Arista User Manual v. 4.6.0 (12/22/2010), at 324.</p>
Command	Description									
show ip mfib	Displays the forwarding entries and interfaces in the IPv4 MFIB									
show ip mfib active	Displays information from the IPv4 MFIB about the rate at which active multicast sources are sending to multicast groups.									
show ip mfib count	Displays a summary of traffic statistics from the IPv4 MFIB about multicast sources and groups.									

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<p>show ip igmp interface</p> <p>To display multicast-related information about an interface, use the <code>show ip igmp interface</code> command in user EXEC or privileged EXEC mode.</p> <p><code>show ip igmp [vrf vrf-name] interface [interface-type interface-number]</code></p> <p>If you omit the optional arguments, the <code>show ip igmp interface</code> command displays information about all interfaces.</p> <p>Cisco IOS Multicast Command Reference at 618 (2013)</p> <p><code>show ip igmp interface</code> Displays multicast-related information about an interface.</p> <p>Cisco IOS Multicast Command Reference (2013), at 12.</p>	<p>show ip igmp interface</p> <p>The <code>show ip igmp interface</code> command displays multicast-related information about an interface.</p> <ul style="list-style-type: none"> • <code>show ip igmp interface</code> – displays all multicast information for all interfaces • <code>show ip igmp interface int-name</code> – displays multicast information for the specified interfaces. <p>When all arguments are omitted, the command displays information for all interfaces.</p> <p>Platform all Command Mode EXEC</p> <p>Command Syntax</p> <p><code>show ip igmp interface [INT_NAME]</code></p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1850.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1558; Arista User Manual, v. 4.11.1 (1/11/13), at 1253; Arista User Manual v. 4.10.3 (10/22/12), at 1038; Arista User Manual v. 4.9.3.2 (5/3/12), at 796; Arista User Manual v. 4.8.2 (11/18/11), at 614; Arista User Manual v. 4.7.3 (7/18/11), at 491; Arista User Manual v. 4.6.0 (12/22/2010), at 337.</p>


Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<p>ip igmp query-interval</p> <p> Note We recommend that you do not change the default IGMP query interval.</p> <p>To configure the frequency at which the IGMP querier sends Internet Group Management Protocol (IGMP) host-query messages from an interface, use the ip igmp query-interval command in interface configuration mode. To restore the default IGMP query interval, use the no form of this command.</p> <p>ip igmp query-interval seconds no ip igmp query-interval</p> <p>Use the ip igmp query-interval command to configure the frequency at which the IGMP querier sends IGMP host-query messages from an interface. The IGMP querier sends query-host messages to discover which multicast groups have members on the attached networks of the router.</p> <p>Cisco IOS Multicast Command Reference (2013), at 118.</p>	<p>ip igmp query-interval</p> <p>The ip igmp query-interval command configures the frequency at which the configuration mode interface, as an IGMP querier, sends host-query messages.</p> <p>An IGMP querier sends query-host messages to discover the multicast groups that have members on networks attached to the interface. The switch implements a default query interval of 125 seconds.</p> <p>The no ip igmp query-interval and default ip igmp query-interval commands reset the IGMP query interval to the default value of 125 seconds by removing the ip igmp query-interval command from <i>running-config</i>.</p> <p>Platform all Command Mode Interface-Ethernet Configuration Interface-Port-Channel Configuration Interface-VLAN Configuration</p> <p>Command Syntax</p> <p>ip igmp query-interval period no ip igmp query-interval default ip igmp query-interval</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1802.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1522; Arista User Manual, v. 4.11.1 (1/11/13), at 1219; Arista User Manual v. 4.10.3 (10/22/12), at 1028; Arista User Manual v. 4.9.3.2 (5/3/12), at 786; Arista User Manual v. 4.8.2 (11/18/11), at 605; Arista User Manual v. 4.7.3 (7/18/11), at 485; Arista User Manual v. 4.6.0 (12/22/2010), at 331.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<p>ip msdp mesh-group</p> <p>To configure a Multicast Source Discovery Protocol (MSDP) peer to be a member of a mesh group, use the <code>ip msdp mesh-group</code> command in global configuration mode. To remove an MSDP peer from a mesh group, use the <code>no</code> form of this command.</p> <pre>ip msdp [vrf vrf-name] mesh-group mesh-name {peer-address peer-name} no ip msdp [vrf vrf-name] mesh-group mesh-name {peer-address peer-name}</pre> <p>Cisco IOS Multicast Command Reference (2013), at 225</p> <p>A mesh group is a group of MSDP speakers that have fully meshed MSDP connectivity among themselves. Source-Active (SA) messages received from a peer in a mesh group are not forwarded to other peers in the same mesh group.</p> <p>Cisco IOS Multicast Command Reference (2013), at 226.</p>	<p>ip msdp mesh-group</p> <p>The <code>ip msdp mesh-group</code> command configures the specified MSDP peer connection as an MSDP mesh group member. A peer can be assigned to multiple mesh groups. Multiple MSDP peers can be assigned to a common mesh group.</p> <p>An MSDP mesh group is a network of MSDP speakers where each speaker is directly connected to every other speaker. Source-Active (SA) messages that are received from a peer in a mesh group are not forwarded to other peers in that mesh group.</p> <p>The <code>no ip msdp mesh-group</code> and default <code>ip msdp mesh-group</code> commands delete the specified peer connection from a mesh group by remove the corresponding <code>ip msdp mesh-group</code> command from running-config. Commands that do not include a specific MSDP peer deletes all configured connections from the specified mesh group.</p> <p>Platform <code>all</code> Command Mode <code>Global Configuration</code></p> <p>Command Syntax</p> <pre>ip msdp mesh-group group_name peer_id no ip msdp mesh-group group_name [peer_id] default ip msdp mesh-group group_name [peer_id]</pre> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1928.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1634; Arista User Manual, v. 4.11.1 (1/11/13), at 1325.</p>
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<p>Use the <code>ip multicast multipath</code> command to enable load splitting of IP multicast traffic across multiple equal-cost paths.</p> <p>If two or more equal-cost paths from a source are available, unicast traffic will be load split across those paths. However, by default, multicast traffic is not load split across multiple equal-cost paths. In general, multicast traffic flows down from the reverse path forwarding (RPF) neighbor. According to the Protocol Independent Multicast (PIM) specifications, this neighbor must have the highest IP address if more than one neighbor has the same metric.</p> <p>Configuring load splitting with the <code>ip multicast multipath</code> command causes the system to load split multicast traffic across multiple equal-cost paths based on source address using the S-hash algorithm. When the <code>ip multicast multipath</code> command is configured and multiple equal-cost paths exist, the path in which multicast traffic will travel is selected based on the source IP address. Multicast traffic from different sources will be load split across the different equal-cost paths. Load splitting will not occur across equal-cost paths for multicast traffic from the same source sent to different multicast groups.</p> <p>Cisco IOS Multicast Command Reference (2013), at 284.</p>	<p>Equal Cost Multipath Routing (ECMP) and Load Sharing</p> <p>Multiple routes that have identical destinations and administrative distances comprise an Equal Cost Multi-Path (ECMP) route. The switch attempts to spread traffic to all ECMP route paths equally.</p> <p>If two or more equal-cost paths from a source are available, unicast traffic is load split across those paths. By default, multicast traffic is not load split. Multicast traffic generally flows from the reverse path forwarding (RPF) neighbor and, according to Protocol Independent Multicast (PIM) specifications, the neighbor with the highest IP address has precedence when multiple neighbors have the same metric.</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1231.</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 1191; Arista User Manual v. 4.12.3 (7/17/13), at 1042; Arista User Manual, v. 4.11.1 (1/11/13), at 398; Arista User Manual v. 4.10.3 (10/22/12), at 330.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<p>Enabling PIM on an interface also enables Internet Group Management Protocol (IGMP) operation on that interface. An interface can be configured to be in dense mode, passive mode, sparse mode, or sparse-dense mode. The mode describes how the Cisco IOS software populates its multicast routing table and how the software forwards multicast packets that it receives from its directly connected LANs. Dense mode interfaces are always added to the table when the multicast routing table is populated. Sparse mode interfaces are added to the table only when periodic join messages are received from downstream routers, or there is a directly connected member on the interface.</p> <p>Cisco IOS Multicast Command Reference (2013), at 330.</p>	<p>Enabling IGMP</p> <p>Enabling PIM on an interface also enables IGMP on that interface. When the switch populates the multicast routing table, interfaces are added to the table only when periodic join messages are received from downstream routers, or when there is a directly connected member on the interface.</p> <p>By default, PIM and IGMP are disabled on an interface. The <code>ip pim sparse-mode</code> command enables PIM and IGMP on the configuration mode interface.</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1778.</p> <p><i>See also</i> Arista User Manual v. 4.13.6F (4/14/2014), at 1726; Arista User Manual v. 4.12.3 (7/17/13), at 1504; Arista User Manual, v. 4.11.1 (1/11/13), at 1204; Arista User Manual v. 4.10.3 (10/22/12), at 998; Arista User Manual v. 4.9.3.2 (5/3/12), at 756; Arista User Manual v. 4.8.2 at 578; Arista User Manual v. 4.7.3 (7/18/11), at 458; Arista User Manual v. 4.6.0 (12/22/2010), at 308.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<p>ip pim sparse sg-expiry-timer</p> <p>To adjust the (S, G) expiry timer interval for Protocol Independent Multicast sparse mode (PIM-SM) (S, G) multicast routes (mroutes), use the ip pim sparse sg-expiry-timer command in global configuration mode. To restore the default setting with respect to this command, use the no form of this command.</p> <p>ip pim [vrf vrf-name] sparse sg-expiry-timer seconds [sg-list access-list] no ip pim [vrf vrf-name] sparse sg-expiry-timer</p> <p>Cisco IOS Multicast Command Reference (2013), at 405.</p> <p>Use the ip pim sparse sg-expiry-timer command to adjust the expiry timer interval for PIM-SM (S, G) mroute entries to a time value greater than the default expiry timer interval of 180 seconds. This command can be used to lock down the shortest-path tree (SPT) for intermittent sources in PIM-SM network environments, such as sources in trading floor environments that sporadically send financial data streams to multicast groups during trading floor hours.</p> <p>When a source stops sending traffic to a multicast group, the corresponding (S, G) mroute entry eventually times out and the (S, G) entry is removed. When the source resumes sending traffic to the group, the (S, G) entry is rebuilt. During the short time interval before the (S, G) entry is rebuilt, the traffic is forwarded on the (*, G) forwarding entry. There is a small window of time before the (S, G) entry is completely built in which packets may be dropped. The ip pim sparse sg-expiry-timer command can be used to maintain the (S, G) entry so that it will not be removed and the stream will not potentially suffer packet loss.</p> <p>Cisco IOS Multicast Command Reference(2013), at 406.</p>	<p>ip pim sparse-mode sg-expiry-timer</p> <p>The ip pim sparse-mode sg-expiry-timer command adjusts the (S, G) expiry timer interval for PIM-SM (S, G) multicast routes (mroutes). This command locks the shortest-path tree (SPT) for intermittent PIM-SM sources. The command does not apply to (*, G) mroutes.</p> <p>When a source stops sending traffic to a multicast group, the corresponding (S, G) mroute is removed upon timer expiry. When the source resumes sending traffic to the group, the (S, G) entry is rebuilt. Before the (S, G) entry is rebuilt, traffic is forwarded on the (*, G) forwarding entry. Packets may be dropped before the (S, G) entry is completely built. The ip pim sparse-mode sg-expiry-timer command maintains the (S, G) entry, avoiding its removal and preventing packet loss.</p> <p>The no ip pim sparse-mode sg-expiry-timer and default ip pim sparse-mode sg-expiry-timer commands restore the default setting of 210 seconds by deleting the ip pim sparse-mode sg-expiry-timer statement from <i>running-config</i>.</p> <p>Platform all Command Mode Global Configuration</p> <p>Command Syntax</p> <p>ip pim sparse-mode sg-expiry-timer period no ip pim sparse-mode sg-expiry-timer default ip pim sparse-mode sg-expiry-timer</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1896.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1602; Arista User Manual, v. 4.11.1 (1/11/13), at 1297; Arista User Manual v. 4.10.3 (10/22/12), at 1091; Arista User Manual v. 4.9.3.2 (5/3/12), at 848; Arista User Manual v. 4.8.2 (11/18/11), at 646; Arista User Manual v. 4.7.3 (7/18/11), at 516; Arista User Manual v. 4.6.0 (12/22/2010), at 361.</p>

Copyright Registration Information	Cisco	Arista								
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<table><tr><th>Command</th><th>Description</th></tr><tr><td>ip host</td><td>Defines a static host name-to-address mapping in the host cache.</td></tr><tr><td>mls rp ip multicast</td><td>Enables IP multicast MLS (hardware switching) on an external or internal router in conjunction with Layer 3 switching hardware for the Catalyst 5000 switch.</td></tr><tr><td>show ip mroute</td><td>Displays the contents of the IP multicast routing table</td></tr></table> <p>Cisco IOS Multicast Command Reference (2013), at 21.</p>	Command	Description	ip host	Defines a static host name-to-address mapping in the host cache.	mls rp ip multicast	Enables IP multicast MLS (hardware switching) on an external or internal router in conjunction with Layer 3 switching hardware for the Catalyst 5000 switch.	show ip mroute	Displays the contents of the IP multicast routing table	<p>show ip mroute count</p> <p>The show ip mroute count command displays IP multicast routing table statistics, including number of packets, packets per second, average packet size, and bits per second.</p> <p>The show ip mroute command displays the contents of the IP multicast routing table.</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1773</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1500; Arista User Manual, v. 4.11.1 (1/11/13), at 1199; Arista User Manual v. 4.10.3 (10/22/12), at 1023; Arista User Manual v. 4.9.3.2 (5/3/12), at 781; Arista User Manual v. 4.8.2 (11/18/11), at 600; Arista User Manual v. 4.7.3 (7/18/11), at 479; Arista User Manual v. 4.6.0 (12/22/2010), at 326.</p>
Command	Description									
ip host	Defines a static host name-to-address mapping in the host cache.									
mls rp ip multicast	Enables IP multicast MLS (hardware switching) on an external or internal router in conjunction with Layer 3 switching hardware for the Catalyst 5000 switch.									
show ip mroute	Displays the contents of the IP multicast routing table									
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<p>show ip igmp snooping</p> <p>To display the Internet Group Management Protocol (IGMP) snooping configuration of a device, use the show ip igmp snooping command in user EXEC or privileged EXEC mode.</p> <p>show ip igmp snooping [groups [count] vlan vlan-id [ip-address] count]] mrouter [[vlan vlan-id]] [bd bd-id]] [querier] [vlan vlan-id] bd bd-id]</p> <p>Cisco IOS Multicast Command Reference at 625 (2013).</p> <p>The following is sample output from the show ip igmp snooping command:</p> <pre>Router# show ip igmp snooping Global IGMP Snooping configuration: ----- IGMP snooping : Enabled IGMPv3 snooping (minimal) : Enabled Report suppression : Enabled TCN solicit query : Disabled TCN flood query count : 2 Last Member Query Interval : 1000</pre> <p>IOS Multicast Command Reference (2013), at 625.</p>	<p>IGMP Snooping Status</p> <p>The show ip igmp snooping command displays the Internet Group Management Protocol (IGMP) snooping configuration of a device.</p> <p>Example</p> <ul style="list-style-type: none">This command displays the switch's IGMP snooping configuration. <pre>switch>show ip igmp snooping Global IGMP Snooping configuration: ----- IGMP snooping : Enabled Robustness variable : 2</pre> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1785.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1511; Arista User Manual, v. 4.11.1 (1/11/13), at 1255; Arista User Manual v. 4.10.3 (10/22/12), at 1066; Arista User Manual v. 4.9.3.2 (5/3/12), at 824; Arista User Manual v. 4.8.2 (11/18/11), at 630; Arista User Manual v. 4.7.3 (7/18/11), at 505; Arista User Manual v. 4.6.0 (12/22/2010), at 351.</p>								

Copyright Registration Information	Cisco	Arista						
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<p>show ip igmp snooping mrouter</p> <p> Note The documentation for this command has been integrated into the documentation for the show ip igmp snooping command. Please see the show ip igmp snooping command for complete and up-to-date information about displaying information for dynamically learned and manually configured multicast router ports.</p> <p>To display information on dynamically learned and manually configured multicast router ports, use the show ip igmp snooping mrouter command in privileged EXEC mode.</p> <p>show ip igmp snooping mrouter {<i>vlan</i> <i>vlan-id</i>} [<i>bd</i> <i>bd-id</i>]</p> <table border="1"> <tr> <td>Syntax Description</td><td>vlan <i>vlan-id</i></td><td>Specifies a VLAN. Valid values are 1 to 1001.</td></tr> <tr> <td></td><td>bd <i>bd-id</i></td><td>Specifies a bridge domain. Valid values are 1 to 16823.</td></tr> </table> <p>Cisco IOS Multicast Command Reference (2013), at 634.</p>	Syntax Description	vlan <i>vlan-id</i>	Specifies a VLAN. Valid values are 1 to 1001.		bd <i>bd-id</i>	Specifies a bridge domain. Valid values are 1 to 16823.	<p>show ip igmp snooping mrouter</p> <p>The show ip igmp snooping mrouter command displays information on dynamically learned and manually configured multicast router ports. Command provides options to include only specific VLANs.</p> <p>Platform all Command Mode EXEC</p> <p>Command Syntax</p> <p>show ip igmp snooping mrouter [<i>VLAN_ID</i>] [<i>DATA</i>]</p> <p>Parameters</p> <ul style="list-style-type: none"> VLAN_ID specifies VLAN for which command displays information. Options include: <ul style="list-style-type: none"> <no parameter> all VLANs. <i>vlan v_num</i> specified VLAN. DATA specifies the type of information displayed. Options include: <ul style="list-style-type: none"> <no parameter> displays VLAN number and port-list for each group. <i>detail</i> displays port-specific data for each group; includes transmission times and expiration. <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1859</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1567; Arista User Manual, v. 4.11.1 (1/11/13), at 1262; Arista User Manual v. 4.10.3 (10/22/12), at 1073; Arista User Manual v. 4.9.3.2 (5/3/12), at 830; Arista User Manual v. 4.8.2 (11/18/11), at 636; Arista User Manual v. 4.7.3 (7/18/11), at 511.</p>
Syntax Description	vlan <i>vlan-id</i>	Specifies a VLAN. Valid values are 1 to 1001.						
	bd <i>bd-id</i>	Specifies a bridge domain. Valid values are 1 to 16823.						

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<p>show ip mfib</p> <p>To display the forwarding entries and interfaces in the IPv4 Multicast Forwarding Information Base (MFIB), use the show ip mfib command in user EXEC or privileged EXEC mode.</p> <p>show ip mfib [vrf {vrf-name *}] [all linkscope] group-address/mask group-address [source-address] source-address group-address] [verbose]</p> <p>Cisco IOS Multicast Command Reference (2013) at 649.</p>	<p>show ip mfib</p> <p>The show ip mfib command displays the forwarding entries and interfaces in the IPv4 Multicast Forwarding Information Base (MFIB) for hardware forwarded routes. Parameters options are available to filter output by group address or group and source addresses</p> <p>Platform all Command Mode EXEC</p> <p>Command Syntax</p> <p>show ip mfib [ROUTE]</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1770</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1497; Arista User Manual, v. 4.11.1 (1/11/13), at 1196; Arista User Manual v. 4.10.3 (10/22/12), at 1020; Arista User Manual v. 4.9.3.2 (5/3/12), at 778; Arista User Manual v. 4.8.2 (11/18/11), at 597; Arista User Manual v. 4.7.3 (7/18/11), at 477; Arista User Manual v. 4.6.0 (12/22/2010), at 324.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<p>snmp-server enable traps pim</p> <p>To enable Protocol Independent Multicast (PIM) Simple Network Management Protocol (SNMP) notifications, use the snmp-server enable traps pim command in global configuration mode. To disable PIM-specific SNMP notifications, use the no form of this command.</p> <p>snmp-server enable traps pim [<i>neighbor-change</i>] [<i>rp-mapping-change</i>] [<i>invalid-pim-message</i>]</p> <p>no snmp-server enable traps pim</p> <p>Cisco IOS Multicast Command Reference (2013), at 950.</p> <p>SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types. PIM notifications are defined in the CISCO-PIM-MIB.mib and PIM-MIB.mib files, available from Cisco.com at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.</p> <p>Cisco IOS Multicast Command Reference (2013), at 951.</p>	<p>snmp-server enable traps</p> <p>The snmp-server enable traps command enables the transmission of Simple Network Management Protocol (SNMP) notifications as traps or inform requests. This command enables both traps and inform requests for the specified notification types. The snmp-server host command specifies the notification type (traps or informs). Sending notifications requires at least one snmp-server host command.</p> <p>The snmp-server enable traps and no snmp-server enable traps commands, without an MIB parameter, specifies the default notification trap generation setting for all MIBs. These commands, when specifying an MIB, controls notification generation for the specified MIB. The default snmp-server enable traps command resets notification generation to the default setting for the specified MIB.</p> <p>Platform all Command Mode Global Configuration</p> <p>Command Syntax</p> <p>snmp-server enable traps [<i>trap_type</i>] no snmp-server enable traps [<i>trap_type</i>] default snmp-server enable traps [<i>trap_type</i>]</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1990.</p> <p><i>See also</i> Arista User Manual v. 4.13.6F (4/14/2014), at 1918; Arista User Manual v. 4.12.3 (7/17/13), at 1680; Arista User Manual, v. 4.11.1 (1/11/13), at 1365; Arista User Manual v. 4.10.3 (10/22/12), at 1132; Arista User Manual v. 4.9.3.2 (5/3/12), at 888; Arista User Manual v. 4.8.2 at 696; Arista User Manual v. 4.7.3 (7/18/11), at 552.</p>


Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<p>lacp port-priority</p> <p>To set the priority for a physical interface, use the lacp port-priority command in interface configuration mode. To return to the default setting, use the no form of this command.</p> <p>lacp port-priority priority</p> <p>no lacp port-priority</p> <p>Cisco IOS Interfaces and Hardware Component Command Reference (2013), at 690.</p> <p>You may assign a port priority to each port on a device running Link Aggregation Control Protocol (LACP). You can specify the port priority by using the lacp port-priority command at the command-line interface (CLI) or use the default port priority (32768) that is carried as part of the LACP protocol data unit (PDU) exchanged with the partner. Port priority is used to decide which ports should be put in standby mode when a hardware limitation or the lacp max-bundle command configuration prevents all compatible ports from aggregating. Priority is supported only on port channels with LACP-enabled physical interfaces.</p> <p>Cisco IOS Interfaces and Hardware Component Command Reference (2013), at 691.</p>	<p>Configuring Port Priority</p> <p>LACP port priority determines the port that is active in a LAG in fallback mode. Numerically lower values have higher priority. Priority is supported on port channels with LACP-enabled physical interfaces.</p> <p>The lacp port-priority command sets the aggregating port priority for the configuration mode interface.</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 461.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 395; Arista User Manual, v. 4.11.1 (1/11/13), at 333; Arista User Manual v. 4.10.3 (10/22/12), at 291; Arista User Manual v. 4.9.3.2 (5/3/12), at 275; Arista User Manual v. 4.8.2 (11/18/11), at 207.</p>

Copyright Registration Information	Cisco	Arista						
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<div>priority1</div> <p>To set a preference level for a Precision Time Protocol clock, use the <code>priority1</code> command in PTP clock configuration mode. To remove a <code>priority1</code> configuration, use the <code>no</code> form of this command.</p> <p><code>priority1 priorityvalue</code> <code>no priority1 priorityvalue</code></p> <p>...</p> <div>Usage Guidelines<div>Slave devices use the <code>priority1</code> value when selecting a master clock. The <code>priority1</code> value has precedence over the <code>priority2</code> value.</div></div> <p>Cisco IOS Interfaces and Hardware Component Command Reference (2013), at 1003.</p>	<div>ptp priority1</div> <p>The <code>ptp priority1</code> command configures the <code>priority1</code> value to use when advertising the clock. This value overrides the default criteria for best master clock selection. Lower values take precedence. The range is from 0 to 255. To remove PTP settings, use the <code>no</code> form of this command.</p> <p>Platform Arad, FM6000 Command Mode Global Configuration</p> <p>Command Syntax</p> <p><code>ptp priority1 priority_rate</code> <code>no ptp priority1</code> <code>default ptp priority1</code></p> <p>Parameters</p> <ul style="list-style-type: none"><code>priority_rate</code> The value to override the default criteria (clock quality, clock class, etc.) for best master clock selection. Lower values take precedence. Value ranges from 0 to 255. The default is 128. <p>Examples</p> <ul style="list-style-type: none">This command configures the preference level for a clock; slave devices use the <code>priority1</code> value when selecting a master clock. <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 326.</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 318; Arista User Manual v. 4.12.3 (7/17/13), at 262; Arista User Manual, v. 4.11.1 (1/11/13), at 208.</p>						
	Cisco IOS 15.4 Effective date of registration: 11/26/2014	<table><tr><th>Command</th><th>Description</th></tr><tr><td><code>link state track</code></td><td>Configures the link state tracking number.</td></tr><tr><td>link state group</td><td>Configures the link state group and interface, as either an upstream or downstream interface in the group.</td></tr></table> <p>Cisco IOS Interfaces and Hardware Component Command Reference (2013), at 1950.</p>	Command	Description	<code>link state track</code>	Configures the link state tracking number.	link state group	Configures the link state group and interface, as either an upstream or downstream interface in the group.
Command	Description							
<code>link state track</code>	Configures the link state tracking number.							
link state group	Configures the link state group and interface, as either an upstream or downstream interface in the group.							


Copyright Registration Information	Cisco	Arista																																																											
	<div><div>show interfaces transceiver</div><div>To display information about the optical transceivers that have digital optical monitoring (DOM) enabled, use the <code>show interfaces transceiver</code> command in privileged EXEC mode.</div><div>Catalyst 6500 Series Switches and Cisco 7600 Series Routers</div><div>show interfaces [interface interface-number] transceiver [threshold violations] properties [detail module number]</div><div>Cisco 7200 VXR</div><div>show interfaces [interface interface-number] transceiver</div><div>Cisco ASR 901 Routers</div><div>show interfaces [interface interface-number] transceiver [threshold {table violations} detail supported-list]</div></div> <div>Cisco IOS Interfaces and Hardware Component Command Reference (2013), at 1878.</div> <div><div>Examples</div><div>This example shows how to display transceiver information:</div><div><div>Router# show interfaces transceiver</div><div>If device is externally calibrated, only calibrated values are printed.</div><div>++ : high alarm, + : high warning, - : low warning, -- : low alarm.</div><div>NA or N/A: not applicable, Tx: transmit, Rx: receive.</div><div>mA: milliamperes, dBm: decibels (milliwatts).</div><table><thead><tr><th>Port</th><th>Temperature (Celsius)</th><th>Voltage (Volts)</th><th>Current (mA)</th><th>Optical Tx Power (dBm)</th><th>Optical Rx Power (dBm)</th></tr></thead><tbody><tr><td>Gi1/1</td><td>40.6</td><td>5.09</td><td>0.4</td><td>-25.2</td><td>N/A</td></tr><tr><td>Gi2/1</td><td>35.6</td><td>5.06</td><td>0.1</td><td>-29.2</td><td>N/A</td></tr><tr><td>Gi2/2</td><td>49.6</td><td>3.30</td><td>0.0</td><td>7.1</td><td>-16.7</td></tr></tbody></table></div></div> <div>Cisco IOS 15.4</div> <div>Effective date of registration: 11/26/2014</div>	Port	Temperature (Celsius)	Voltage (Volts)	Current (mA)	Optical Tx Power (dBm)	Optical Rx Power (dBm)	Gi1/1	40.6	5.09	0.4	-25.2	N/A	Gi2/1	35.6	5.06	0.1	-29.2	N/A	Gi2/2	49.6	3.30	0.0	7.1	-16.7	<div><div>show interfaces transceiver</div><div>The <code>show interfaces transceiver</code> command displays operational transceiver data for the specified interfaces.</div><div>Platform all</div><div>Command Mode EXEC</div><div>Command Syntax</div><div>show interfaces [INTERFACE] transceiver [DATA_FORMAT]</div><div>...</div><div>Examples</div><div><ul style="list-style-type: none">This command displays transceiver data on Ethernet interfaces 1 through 4.</div><div><div>switch>show interfaces ethernet 1-4 transceiver</div><div>If device is externally calibrated, only calibrated values are printed.</div><div>N/A: not applicable, Tx: transmit, Rx: receive.</div><div>mA: milliamperes, dBm: decibels (milliwatts).</div><table><thead><tr><th>Port</th><th>Temp (Celsius)</th><th>Voltage (Volts)</th><th>Bias Current (mA)</th><th>Optical Tx Power (dBm)</th><th>Optical Rx Power (dBm)</th><th>Last Update (Date Time)</th></tr></thead><tbody><tr><td>E1</td><td>34.17</td><td>3.30</td><td>6.75</td><td>-2.41</td><td>-2.83</td><td>2011-12-02 16:18:48</td></tr><tr><td>E2</td><td>35.08</td><td>3.30</td><td>6.75</td><td>-2.23</td><td>-2.06</td><td>2011-12-02 16:18:42</td></tr><tr><td>E3</td><td>36.72</td><td>3.30</td><td>7.20</td><td>2.02</td><td>2.14</td><td>2011-12-02 16:18:49</td></tr><tr><td>E4</td><td>35.91</td><td>3.30</td><td>6.92</td><td>-2.20</td><td>-2.23</td><td>2011-12-02 16:18:45</td></tr></tbody></table><div>switch></div></div></div> <div>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 451.</div> <div>See also Arista User Manual v. 4.12.3 (7/17/13), at 385; Arista User Manual, v. 4.11.1 (1/11/13), at 326; Arista User Manual v. 4.10.3 (10/22/12), at 284; Arista User Manual v. 4.9.3.2 (5/3/12), at 266.</div>	Port	Temp (Celsius)	Voltage (Volts)	Bias Current (mA)	Optical Tx Power (dBm)	Optical Rx Power (dBm)	Last Update (Date Time)	E1	34.17	3.30	6.75	-2.41	-2.83	2011-12-02 16:18:48	E2	35.08	3.30	6.75	-2.23	-2.06	2011-12-02 16:18:42	E3	36.72	3.30	7.20	2.02	2.14	2011-12-02 16:18:49	E4	35.91	3.30	6.92	-2.20	-2.23	2011-12-02 16:18:45
Port	Temperature (Celsius)	Voltage (Volts)	Current (mA)	Optical Tx Power (dBm)	Optical Rx Power (dBm)																																																								
Gi1/1	40.6	5.09	0.4	-25.2	N/A																																																								
Gi2/1	35.6	5.06	0.1	-29.2	N/A																																																								
Gi2/2	49.6	3.30	0.0	7.1	-16.7																																																								
Port	Temp (Celsius)	Voltage (Volts)	Bias Current (mA)	Optical Tx Power (dBm)	Optical Rx Power (dBm)	Last Update (Date Time)																																																							
E1	34.17	3.30	6.75	-2.41	-2.83	2011-12-02 16:18:48																																																							
E2	35.08	3.30	6.75	-2.23	-2.06	2011-12-02 16:18:42																																																							
E3	36.72	3.30	7.20	2.02	2.14	2011-12-02 16:18:49																																																							
E4	35.91	3.30	6.92	-2.20	-2.23	2011-12-02 16:18:45																																																							

Copyright Registration Information	Cisco	Arista				
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<p>aaa authentication dot1x</p> <p>To specify one or more authentication, authorization, and accounting (AAA) methods for use on interfaces running IEEE 802.1X, use the aaa authentication dot1x command in global configuration mode. To disable authentication, use the no form of this command.</p> <pre>aaa authentication dot1x {default listname} method1 [method2 ...] no aaa authentication dot1x {default listname} method1 [method2 ...]</pre> <p>Cisco IOS Security Command Reference: Commands A to C (2013), at 54.</p>	<p>Example</p> <ul style="list-style-type: none">The aaa authentication dot1x command specifies one or more authentication, authorization, and accounting (AAA) methods for use on interfaces running IEEE 802.1X. The following example uses the aaa authentication dot1x command with RADIUS authentication. <pre>switch(config)# aaa authentication dot1x default group radius switch(config)#</pre> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 557.</p>				
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<table><tr><th>Command</th><th>Description</th></tr><tr><td>show dot1x (EtherSwitch)</td><td>Displays 802.1X statistics, administrative status, and operational status for the switch or for the specified interface.</td></tr></table> <p>Cisco IOS Security Command Reference: Commands A to C (2013), at 56.</p>	Command	Description	show dot1x (EtherSwitch)	Displays 802.1X statistics, administrative status, and operational status for the switch or for the specified interface.	<p>show dot1x</p> <p>The show dot1x command displays the 802.1x statistics, administrative status, and operational status for the specified interface.</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 572.</p>
Command	Description					
show dot1x (EtherSwitch)	Displays 802.1X statistics, administrative status, and operational status for the switch or for the specified interface.					
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<p>Method lists are specific to the type of authorization being requested. AAA supports five different types of authorization:</p> <ul style="list-style-type: none">Commands --Applies to the EXEC mode commands a user issues. Command authorization attempts authorization for all EXEC mode commands, including global configuration commands, associated with a specific privilege level.EXEC --Applies to the attributes associated with a user EXEC terminal session. <p>Cisco IOS Security Command Reference: Commands A to C (2013), at 83.</p>	<p>The switch supports two types of accounting:</p> <ul style="list-style-type: none">EXEC: Provides information about user CLI sessions.Commands: Applies to the CLI commands a user issues. Command authorization attempts authorization for all commands, including configuration commands, associated with a specific privilege level. <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 207.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 154; Arista User Manual, v. 4.11.1 (1/11/13), at 114; Arista User Manual v. 4.10.3 (10/22/12), at 106; Arista User Manual v. 4.9.3.2 (5/3/12), at 93; Arista User Manual v. 4.8.2 (11/18/11), at 87; Arista User Manual v. 4.7.3 (7/18/11), at 73.</p>				

Copyright Registration Information	Cisco	Arista						
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<table><tr><td>auto</td><td>Enables port-based authentication and causes the port to begin in the unauthorized state, allowing only Extensible Authentication Protocol over LAN (EAPOL) frames to be sent and received through the port.</td></tr><tr><td>force-authorized</td><td>Disables IEEE 802.1X on the interface and causes the port to change to the authorized state without requiring any authentication exchange. The port transmits and receives normal traffic without 802.1X-based authentication of the client. The force-authorized keyword is the default.</td></tr><tr><td>force-unauthorized</td><td>Denies all access through this interface by forcing the port to change to the unauthorized state, ignoring all attempts by the client to authenticate.</td></tr></table>	auto	Enables port-based authentication and causes the port to begin in the unauthorized state, allowing only Extensible Authentication Protocol over LAN (EAPOL) frames to be sent and received through the port.	force-authorized	Disables IEEE 802.1X on the interface and causes the port to change to the authorized state without requiring any authentication exchange. The port transmits and receives normal traffic without 802.1X-based authentication of the client. The force-authorized keyword is the default.	force-unauthorized	Denies all access through this interface by forcing the port to change to the unauthorized state, ignoring all attempts by the client to authenticate.	<p>The <code>dot1x port-control force-authorized</code> command causes the port to transition to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1X-based authentication of the client.</p> <p>Example</p> <ul style="list-style-type: none">This example of the command designates Ethernet 1 as an authenticator port that is to continue to forward packets. <pre>switch(config)#interface ethernet 1 switch(config-if-Et1)#dot1x port-control force-authorized switch(config-if-Et1)#</pre> <p>Example</p> <ul style="list-style-type: none">The <code>dot1x port-control force-unauthorized</code> command places the specified ports in the state of unauthorized, denying any access requests from users of the ports. <pre>switch(config)#interface ethernet 1 switch(config-if-Et1)#dot1x port-control force-authorized switch(config-if-Et1)#</pre>
	auto	Enables port-based authentication and causes the port to begin in the unauthorized state, allowing only Extensible Authentication Protocol over LAN (EAPOL) frames to be sent and received through the port.						
force-authorized	Disables IEEE 802.1X on the interface and causes the port to change to the authorized state without requiring any authentication exchange. The port transmits and receives normal traffic without 802.1X-based authentication of the client. The force-authorized keyword is the default.							
force-unauthorized	Denies all access through this interface by forcing the port to change to the unauthorized state, ignoring all attempts by the client to authenticate.							
	Cisco IOS Security Command Reference: Commands A to C (2013), at 354.	Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 558.						

Copyright Registration Information	Cisco	Arista								
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<h3>authentication port-control</h3> <p>To configure the authorization state of a controlled port, use the authentication port-control command in interface configuration mode. To disable the port-control value, use the no form of this command.</p> <p> Note Effective with Cisco IOS Release 12.2(33)SXI, the authentication port-control command replaces the dot1x port-control command.</p> <div>authentication port-control {auto force-authorized force-unauthorized} no authentication port-control</div> <table><tr><th>Syntax Description</th><th></th></tr><tr><td>auto</td><td>Enables port-based authentication and causes the port to begin in the unauthorized state, allowing only Extensible Authentication Protocol over LAN (EAPOL) frames to be sent and received through the port</td></tr><tr><td>force-authorized</td><td>Disables IEEE 802.1X on the interface and causes the port to change to the authorized state without requiring any authentication exchange. The port transmits and receives normal traffic without 802.1X-based authentication of the client. The force-authorized keyword is the default.</td></tr><tr><td>force-unauthorized</td><td>Denies all access through this interface by forcing the port to change to the unauthorized state, ignoring all attempts by the client to authenticate</td></tr></table>	Syntax Description		auto	Enables port-based authentication and causes the port to begin in the unauthorized state, allowing only Extensible Authentication Protocol over LAN (EAPOL) frames to be sent and received through the port	force-authorized	Disables IEEE 802.1X on the interface and causes the port to change to the authorized state without requiring any authentication exchange. The port transmits and receives normal traffic without 802.1X-based authentication of the client. The force-authorized keyword is the default.	force-unauthorized	Denies all access through this interface by forcing the port to change to the unauthorized state, ignoring all attempts by the client to authenticate	<p>— force-unauthorized places the specified or all ports in the state of unauthorized, denying any access requests from users of the ports.</p> <p>Examples</p> <ul style="list-style-type: none">This command configures the switch to disable 802.1x authentication and directly put the port into the authorized state. This is the default setting.<pre>switch(config)#interface Ethernet 1 switch(config-if-Et1)#dot1x port-control force-authorized switch(config-if-Et1)#</pre>This command configures the switch to disable 802.1x authentication and directly put the port to unauthorized state, ignoring all attempts by the client to authenticate.<pre>switch(config)#interface Ethernet 1 switch(config-if-Et1)#dot1x port-control force-unauthorized switch(config-if-Et1)#</pre> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 567.</p>
	Syntax Description									
	auto	Enables port-based authentication and causes the port to begin in the unauthorized state, allowing only Extensible Authentication Protocol over LAN (EAPOL) frames to be sent and received through the port								
force-authorized	Disables IEEE 802.1X on the interface and causes the port to change to the authorized state without requiring any authentication exchange. The port transmits and receives normal traffic without 802.1X-based authentication of the client. The force-authorized keyword is the default.									
force-unauthorized	Denies all access through this interface by forcing the port to change to the unauthorized state, ignoring all attempts by the client to authenticate									

Copyright Registration Information	Cisco	Arista								
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<div>Related Commands</div> <table><thead><tr><th>Command</th><th>Description</th></tr></thead><tbody><tr><td>dot1x max-req</td><td>Sets the maximum number of times that the device sends an EAP-request/identity frame before restarting the authentication process.</td></tr><tr><td>dot1x re-authentication (EtherSwitch)</td><td>Enables periodic reauthentication of the client for the Ethernet switch network module.</td></tr><tr><td>show dot1x (EtherSwitch)</td><td>Displays the 802.1X statistics, administrative status, and operational status for the device or for the specified interface.</td></tr></tbody></table> <div>Cisco IOS Security Command Reference: Commands D to L (2013), at 219.</div>	Command	Description	dot1x max-req	Sets the maximum number of times that the device sends an EAP-request/identity frame before restarting the authentication process.	dot1x re-authentication (EtherSwitch)	Enables periodic reauthentication of the client for the Ethernet switch network module.	show dot1x (EtherSwitch)	Displays the 802.1X statistics, administrative status, and operational status for the device or for the specified interface.	<div>dot1x max-reauth-req</div> <div>The dot1x max-reauth-req command sets the maximum number of times that the switch retransmits an Extensible Authentication Protocol(EAP)-Request frame of types other than EAP-Request/Identity to the client before restarting the authentication process. Value ranges from 1 to 10. Default value is 2.</div> <div>The no dot1x max-reauth-req and default dot1x max-reauth-req commands restores the default value by deleting the corresponding dot1x max-reauth-req command from running-config.</div> <div>Platformall Command ModeInterface-Ethernet Configuration Interface-Management Configuration</div> <div>Command Syntax<div>dot1x max-reauth-req attempts no dot1x max-reauth-req default dot1x max-reauth-req</div></div> <div>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 565.</div>
	Command	Description								
dot1x max-req	Sets the maximum number of times that the device sends an EAP-request/identity frame before restarting the authentication process.									
dot1x re-authentication (EtherSwitch)	Enables periodic reauthentication of the client for the Ethernet switch network module.									
show dot1x (EtherSwitch)	Displays the 802.1X statistics, administrative status, and operational status for the device or for the specified interface.									
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<div>dot1x pae</div> <div>To set the Port Access Entity (PAE) type, use the dot1x pae command in interface configuration mode. To disable the PAE type that was set, use the no form of this command.</div> <div>dot1x pae [supplicant authenticator both] no dot1x pae [supplicant authenticator both]</div> <div>Syntax Description</div> <table><tbody><tr><td>supplicant</td><td>(Optional) The interface acts only as a supplicant and will not respond to messages that are meant for an authenticator.</td></tr><tr><td>authenticator</td><td>(Optional) The interface acts only as an authenticator and will not respond to any messages meant for a supplicant.</td></tr><tr><td>both</td><td>(Optional) The interface behaves both as a supplicant and as an authenticator and thus will respond to all dot1x messages.</td></tr></tbody></table> <div>Cisco IOS Security Command Reference: Commands D to L (2013), at 195.</div>	supplicant	(Optional) The interface acts only as a supplicant and will not respond to messages that are meant for an authenticator.	authenticator	(Optional) The interface acts only as an authenticator and will not respond to any messages meant for a supplicant.	both	(Optional) The interface behaves both as a supplicant and as an authenticator and thus will respond to all dot1x messages.	<div>dot1x pae authenticator</div> <div>The dot1x pae authenticator command sets the Port Access Entity (PAE) type. The interface acts only as an authenticator and will not respond to any messages meant for a supplicant.</div> <div>The no dot1x pae authenticator and default dot1x pae authenticator commands restore the switch default by deleting the corresponding dot1x pae authenticator command from running-config.</div> <div>Platformall Command ModeInterface-Ethernet Configuration Interface-Management Configuration</div> <div>Command Syntax<div>dot1x pae authenticator no dot1x pae authenticator default dot1x pae authenticator</div></div> <div>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 567.</div>		
	supplicant	(Optional) The interface acts only as a supplicant and will not respond to messages that are meant for an authenticator.								
authenticator	(Optional) The interface acts only as an authenticator and will not respond to any messages meant for a supplicant.									
both	(Optional) The interface behaves both as a supplicant and as an authenticator and thus will respond to all dot1x messages.									

Copyright Registration Information	Cisco	Arista								
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<div><div>dot1x port-control</div><div><div></div><div>Note</div><div>Effective with Cisco IOS Release 12.2(33)SXI, the dot1x port-control command is replaced by the authentication port-control command. See the authentication port-control command for more information.</div></div><div><div>To enable manual control of the authorization state of a controlled port, use the dot1x port-control command in interface configuration mode. To disable the port-control value, use the no form of this command.</div><div><div>dot1x port-control {auto force-authorized force-unauthorized}</div><div>no dot1x port-control</div></div><div><div>Syntax Description</div><table><tr><td>auto</td><td>Enables 802.1X port-based authentication and causes the port to begin in the unauthorized state, allowing only Extensible Authentication Protocol over LAN (EAPOL) frames to be sent and received through the port.</td></tr><tr><td>force-authorized</td><td>Disables 802.1X on the interface and causes the port to change to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1X-based authentication of the client. The force-authorized keyword is the default.</td></tr><tr><td>force-unauthorized</td><td>Denies all access through this interface by forcing the port to change to the unauthorized state, ignoring all attempts by the client to authenticate.</td></tr></table></div></div></div>	auto	Enables 802.1X port-based authentication and causes the port to begin in the unauthorized state, allowing only Extensible Authentication Protocol over LAN (EAPOL) frames to be sent and received through the port.	force-authorized	Disables 802.1X on the interface and causes the port to change to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1X-based authentication of the client. The force-authorized keyword is the default.	force-unauthorized	Denies all access through this interface by forcing the port to change to the unauthorized state, ignoring all attempts by the client to authenticate.	<div><div>The dot1x port-control force-authorized command causes the port to transition to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1X-based authentication of the client.</div><div><div>Example</div><div><ul style="list-style-type: none">This example of the command designates Ethernet 1 as an authenticator port that is to continue to forward packets.<pre>switch(config)#interface ethernet 1 switch(config-if-Et1)#dot1x port-control force-authorized switch(config-if-Et1)#</pre></div><div><div>Example</div><div><ul style="list-style-type: none">The dot1x port-control force-unauthorized command places the specified ports in the state of unauthorized, denying any access requests from users of the ports.<pre>switch(config)#interface ethernet 1 switch(config-if-Et1)#dot1x port-control force-unauthorized switch(config-if-Et1)#</pre></div></div><div><div>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 558.</div></div></div></div>		
	auto	Enables 802.1X port-based authentication and causes the port to begin in the unauthorized state, allowing only Extensible Authentication Protocol over LAN (EAPOL) frames to be sent and received through the port.								
force-authorized	Disables 802.1X on the interface and causes the port to change to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1X-based authentication of the client. The force-authorized keyword is the default.									
force-unauthorized	Denies all access through this interface by forcing the port to change to the unauthorized state, ignoring all attempts by the client to authenticate.									
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<table><tr><th>Command</th><th>Description</th></tr><tr><td>aaa authentication dot1x</td><td>Specifies one or more AAA methods for use on interfaces running IEEE 802.1X.</td></tr><tr><td>aaa new-model</td><td>Enables the AAA access-control model.</td></tr><tr><td>debug dot1x</td><td>Displays 802.1X debugging information.</td></tr></table> <div><div>Cisco IOS Security Command Reference: Commands D to L (2013), at 211.</div></div>	Command	Description	aaa authentication dot1x	Specifies one or more AAA methods for use on interfaces running IEEE 802.1X.	aaa new-model	Enables the AAA access-control model.	debug dot1x	Displays 802.1X debugging information.	<div><div>Example</div><div><ul style="list-style-type: none">The aaa authentication dot1x command specifies one or more authentication, authorization, and accounting (AAA) methods for use on interfaces running IEEE 802.1X. The following example uses the aaa authentication dot1x command with RADIUS authentication.<pre>switch(config)# aaa authentication dot1x default group radius switch(config)#</pre></div><div><div>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 557.</div></div></div>
Command	Description									
aaa authentication dot1x	Specifies one or more AAA methods for use on interfaces running IEEE 802.1X.									
aaa new-model	Enables the AAA access-control model.									
debug dot1x	Displays 802.1X debugging information.									

Copyright Registration Information	Cisco	Arista									
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<p>dot1x timeout (EtherSwitch)</p> <p>To set the number of retry seconds between 802.1X authentication exchanges when an Ethernet switch network module is installed in the router, use the dot1x timeout command in global configuration mode. To return to the default setting, use the no form of this command.</p> <p>dot1x timeout {quiet-period seconds} [re-authperiod seconds] [tx-period seconds] no dot1x timeout {quiet-period seconds} [re-authperiod seconds] [tx-period seconds]</p> <table border="1"> <tr> <td>Syntax Description</td><td>quiet-period seconds</td><td>Specifies the time in seconds that the Ethernet switch network module remains in the quiet state following a failed authentication exchange with the client. The range is from 0 to 65535 seconds. The default is 60 seconds.</td></tr> <tr> <td></td><td>re-authperiod seconds</td><td>Specifies the number of seconds between reauthentication attempts. The range is from 1 to 4294967295. The default is 3600 seconds.</td></tr> <tr> <td></td><td>tx-period seconds</td><td>Time in seconds that the switch should wait for a response to an EAP-request/identity frame from the client before retransmitting the request. The range is from 1 to 65535 seconds. The default is 30 seconds.</td></tr> </table> <p>Cisco IOS Security Command Reference: Commands D to L (2013), at 218.</p>	Syntax Description	quiet-period seconds	Specifies the time in seconds that the Ethernet switch network module remains in the quiet state following a failed authentication exchange with the client. The range is from 0 to 65535 seconds. The default is 60 seconds.		re-authperiod seconds	Specifies the number of seconds between reauthentication attempts. The range is from 1 to 4294967295. The default is 3600 seconds.		tx-period seconds	Time in seconds that the switch should wait for a response to an EAP-request/identity frame from the client before retransmitting the request. The range is from 1 to 65535 seconds. The default is 30 seconds.	<p>dot1x timeout quiet-period</p> <p>The dot1x timeout quiet-period command sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client. The range is 1 to 65535 seconds; the default is 60.</p> <p>When the switch cannot authenticate the client, the switch remains idle for a set period of time and then tries again. You can provide a faster response time to the user by entering a number smaller than the default.</p> <p>The no dot1x timeout quiet-period and default dot1x timeout quiet-period commands restore the default advertisement interval of 60 seconds by removing the corresponding dot1x timeout quiet-period command from <i>running-config</i>.</p> <p>Platform all Command Mode Interface-Ethernet Configuration Interface-Management Configuration</p> <p>Command Syntax</p> <pre>dot1x timeout quiet-period quiet_time no dot1x timeout quiet-period default dot1x timeout quiet-period</pre> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 569.</p>
Syntax Description	quiet-period seconds	Specifies the time in seconds that the Ethernet switch network module remains in the quiet state following a failed authentication exchange with the client. The range is from 0 to 65535 seconds. The default is 60 seconds.									
	re-authperiod seconds	Specifies the number of seconds between reauthentication attempts. The range is from 1 to 4294967295. The default is 3600 seconds.									
	tx-period seconds	Time in seconds that the switch should wait for a response to an EAP-request/identity frame from the client before retransmitting the request. The range is from 1 to 65535 seconds. The default is 30 seconds.									
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<p>dot1x max-reauth-req</p> <p>To set the maximum number of times the authenticator sends an Extensible Authentication Protocol (EAP) request/identity frame (assuming that no response is received) to the client, use the dot1x max-reauth-req command in interface configuration mode. To set the maximum number of times to the default setting of 2, use the no form of this command.</p> <p>dot1x max-reauth-req number no dot1x max-reauth-req</p> <p>Cisco IOS Security Command Reference: Commands D to L (2013), at 185.</p>	<p>11.3.5 Setting the Maximum Number of Times the Authenticator Sends EAP Request</p> <p>The dot1x max-reauth-req command sets the maximum number of times that the switch restarts the authentication process before a port changes to the unauthorized state.</p> <p>Example</p> <ul style="list-style-type: none"> These commands set the maximum number of times the authenticator sends an Extensible Authentication Protocol (EAP) request/identity frame to the client. <pre>switch(config)#interface ethernet 1 switch(config-if-Et1)#dot1x max-reauth-req 4 switch(config-if-Et1)#</pre> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 559.</p>									

Copyright Registration Information	Cisco	Arista												
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<table><thead><tr><th>Command</th><th>Description</th></tr></thead><tbody><tr><td>deny (IPv6)</td><td>Sets deny conditions for an IPv6 access list.</td></tr><tr><td>evaluate (IPv6)</td><td>Nests an IPv6 reflexive access list within an IPv6 access list.</td></tr><tr><td>ipv6 access-list</td><td>Defines an IPv6 access list and enters IPv6 access list configuration mode.</td></tr><tr><td>ipv6 traffic-filter</td><td>Filters incoming or outgoing IPv6 traffic on an interface.</td></tr><tr><td>show ipv6 access-list</td><td>Displays the contents of all current IPv6 access lists.</td></tr></tbody></table> Cisco IOS Security Command Reference: Commands M to R at 440 (2013).	Command	Description	deny (IPv6)	Sets deny conditions for an IPv6 access list.	evaluate (IPv6)	Nests an IPv6 reflexive access list within an IPv6 access list.	ipv6 access-list	Defines an IPv6 access list and enters IPv6 access list configuration mode.	ipv6 traffic-filter	Filters incoming or outgoing IPv6 traffic on an interface.	show ipv6 access-list	Displays the contents of all current IPv6 access lists.	<div>show ipv6 access-lists</div> <div>The show ipv6 access-list command displays the contents of all IPv6 access control lists (ACLs) on the switch. Use the summary option to display only the name of the lists and the number of lines in each list.</div> <div>Platformall Command ModePrivileged EXEC</div> <div>Command Syntax show ipv6 access-list [LIST] [SCOPE]</div> <div>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 904.</div> <div>See also Arista User Manual v. 4.12.3 (7/17/13), at 782; Arista User Manual, v. 4.11.1 (1/11/13), at 611; Arista User Manual v. 4.10.3 (10/22/12), at 525.</div>
Command	Description													
deny (IPv6)	Sets deny conditions for an IPv6 access list.													
evaluate (IPv6)	Nests an IPv6 reflexive access list within an IPv6 access list.													
ipv6 access-list	Defines an IPv6 access list and enters IPv6 access list configuration mode.													
ipv6 traffic-filter	Filters incoming or outgoing IPv6 traffic on an interface.													
show ipv6 access-list	Displays the contents of all current IPv6 access lists.													
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<div>security passwords min-length</div> <div>To ensure that all configured passwords are at least a specified length, use the security passwords min-length command in global configuration mode. To disable this functionality, use the no form of this command.</div> <div>security passwords min-length length no security passwords min-length length</div> <div>...</div> <div>The security passwords min-length command provides enhanced security access to the device by allowing you to specify a minimum password length, eliminating common passwords that are prevalent on most networks, such as "lab" and "cisco." This command affects user passwords, enable passwords and secrets, and line passwords. After this command is enabled, any password that is less than the specified length will not work.</div> <div>Cisco IOS Security Command Reference: Commands S to Z at 37 (2013).</div>	<div>password minimum length (Security Management)</div> <div>The password minimum length command provides enhanced security access to the switch by allowing you to specify a minimum password length, eliminating common passwords that are prevalent on most networks. This command affects user passwords, enable passwords and secrets, and line passwords. After this command is enabled, any password that is less than the specified length will fail.</div> <div>...</div> <div>Command Syntax</div> <div>password minimum length characters no password minimum length default password minimum length</div> <div>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 158.</div>												

Copyright Registration Information	Cisco	Arista								
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<div>show aaa method-lists</div> <div>To display all the named method lists defined in the authentication, authorization, and accounting (AAA) subsystem, use the <code>show aaa method-lists</code> command in user EXEC or privileged EXEC mode.</div> <div>show aaa method-lists {accounting all authentication authorization}</div> <div>Syntax Description</div> <table><tr><td>accounting</td><td>Displays method lists defined for accounting services.</td></tr><tr><td>all</td><td>Displays method lists defined for all services.</td></tr><tr><td>authentication</td><td>Displays method lists defined for authentication services.</td></tr><tr><td>authorization</td><td>Displays method lists defined for authorization services.</td></tr></table> <div>Cisco IOS Security Command Reference: Commands S to Z at 185 (2013).</div>	accounting	Displays method lists defined for accounting services.	all	Displays method lists defined for all services.	authentication	Displays method lists defined for authentication services.	authorization	Displays method lists defined for authorization services.	<div>show aaa method-lists</div> <div>The <code>show aaa method-lists</code> command displays all the named method lists defined in the specified authentication, authorization, and accounting (AAA) service.</div> <div>Platform all</div> <div>Command Mode Privileged EXEC</div> <div>Command Syntax</div> <div>show aaa method-lists SERVICE_TYPE</div> <div>Parameters</div> <div><ul style="list-style-type: none">SERVICE_TYPE the service type of the method lists that the command displays.<ul style="list-style-type: none">accounting accounting services.authentication authentication services.authorization authorization services.all accounting, authentication, and authorization services.</div> <div>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 248.</div> <div>See also Arista User Manual v. 4.12.3 (7/17/13), at 192; Arista User Manual, v. 4.11.1 (1/11/13), at 145; Arista User Manual v. 4.10.3 (10/22/12), at 137; Arista User Manual v. 4.9.3.2 (5/3/12), at 126; Arista User Manual v. 4.8.2 (11/18/11), at 115; Arista User Manual v. 4.7.3 (7/18/11), at 99.</div>
	accounting	Displays method lists defined for accounting services.								
all	Displays method lists defined for all services.									
authentication	Displays method lists defined for authentication services.									
authorization	Displays method lists defined for authorization services.									
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<table><tr><th>Command</th><th>Description</th></tr><tr><td>snmp-server community</td><td>Specifies the community access string to define the relationship between the SNMP manager and the SNMP agent to permit access to SNMP.</td></tr><tr><td>snmp-server host</td><td>Specifies the recipient (host) of an SNMP notification operation.</td></tr></table> <div>Cisco IOS Security Command Reference: Commands S to Z at 1042 (2013).</div>	Command	Description	snmp-server community	Specifies the community access string to define the relationship between the SNMP manager and the SNMP agent to permit access to SNMP.	snmp-server host	Specifies the recipient (host) of an SNMP notification operation.	<div>Configuring the Host</div> <div>The <code>snmp-server host</code> command specifies the recipient of a SNMP notification. An SNMP host is the recipient of an SNMP trap operation. The <code>snmp-server host</code> command sets the community string if it was not previously configured.</div> <div>Arista User Manual v. 4.14.3F (Rev. 2)(10/2/2014), at 1967.</div> <div>See also Arista User Manual v. 4.12.3 (7/17/13), at 1686; Arista User Manual, v. 4.11.1 (1/11/13), at 1344; Arista User Manual v. 4.10.3 (10/22/12), at 1110; Arista User Manual v. 4.9.3.2 (5/3/12), at 866; Arista User Manual v. 4.8.2 (11/18/11), at 677; Arista User Manual v. 4.7.3 (7/18/11), at 533.</div>		
Command	Description									
snmp-server community	Specifies the community access string to define the relationship between the SNMP manager and the SNMP agent to permit access to SNMP.									
snmp-server host	Specifies the recipient (host) of an SNMP notification operation.									

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<p>snmp-server enable traps ipsec</p> <p>To enable the router to send IP Security (IPSec) Simple Network Management Protocol (SNMP) notifications, use the snmp-server enable traps ipsec command in global configuration mode. To disable IPSec SNMP notifications, use the no form of this command.</p> <p>snmp-server enable traps ipsec [cryptomap [add delete attach detach]] [tunnel [start stop]] [too-many-sas]</p> <p>no snmp-server enable traps ipsec [cryptomap [add delete attach detach]] [tunnel [start stop]] [too-many-sas]</p> <p>...</p> <p>SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.</p> <p>Cisco IOS Security Command Reference: Commands S to Z at 1044 - 1045 (2013).</p>	<p>snmp-server enable traps</p> <p>The snmp-server enable traps command enables the transmission of Simple Network Management Protocol (SNMP) notifications as traps or inform requests. This command enables both traps and inform requests for the specified notification types. The snmp-server host command specifies the notification type (traps or informs). Sending notifications requires at least one snmp-server host command.</p> <p>The snmp-server enable traps and no snmp-server enable traps commands, without an MIB parameter, specifies the default notification trap generation setting for all MIBs. These commands, when specifying an MIB, controls notification generation for the specified MIB. The default snmp-server enable traps command resets notification generation to the default setting for the specified MIB.</p> <p>Platform all Command Mode Global Configuration</p> <p>Command Syntax</p> <p>snmp-server enable traps [trap_type] no snmp-server enable traps [trap_type] default snmp-server enable traps [trap_type]</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) at 1990 (October 2, 2014).</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 1918; Arista User Manual v. 4.12.3 (7/17/13), at 1680; Arista User Manual, v. 4.11.1 (1/11/13), at 1365; Arista User Manual v. 4.10.3 (10/22/12), at 1132; Arista User Manual v. 4.9.3.2 (5/3/12), at 888; Arista User Manual v. 4.8.2 at 696; Arista User Manual v. 4.7.3 (7/18/11), at 552.</p>

Copyright Registration Information	Cisco	Arista														
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<table><thead><tr><th>Command</th><th>Description</th></tr></thead><tbody><tr><td>connect</td><td>Logs in to a host that supports Telnet, rlogin, or LAT.</td></tr><tr><td>kerberos clients mandatory</td><td>Causes the rsh, rcp, rlogin, and telnet commands to fail if they cannot negotiate the Kerberos Protocol with the remote server.</td></tr><tr><td>name connection</td><td>Assigns a logical name to a connection.</td></tr><tr><td>rlogin</td><td>Logs in to a UNIX host using rlogin.</td></tr><tr><td>show hosts</td><td>Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses.</td></tr><tr><td>show tcp</td><td>Displays the status of TCP connections.</td></tr></tbody></table> Cisco IOS Security Command Reference: Commands S to Z at 1192 (2013).	Command	Description	connect	Logs in to a host that supports Telnet, rlogin, or LAT.	kerberos clients mandatory	Causes the rsh, rcp, rlogin, and telnet commands to fail if they cannot negotiate the Kerberos Protocol with the remote server.	name connection	Assigns a logical name to a connection.	rlogin	Logs in to a UNIX host using rlogin.	show hosts	Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses.	show tcp	Displays the status of TCP connections.	show hosts The show hosts command displays the default domain name, name lookup service style, a list of name server hosts, and the static hostname-IP address maps. Platform all Command Mode EXEC Command Syntax show hosts Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 342. <i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 276; Arista User Manual, v. 4.11.1 (1/11/13), at 222; Arista User Manual v. 4.10.3 (10/22/12), at 191; Arista User Manual v. 4.9.3.2 (5/3/12), at 177.
Command	Description															
connect	Logs in to a host that supports Telnet, rlogin, or LAT.															
kerberos clients mandatory	Causes the rsh, rcp, rlogin, and telnet commands to fail if they cannot negotiate the Kerberos Protocol with the remote server.															
name connection	Assigns a logical name to a connection.															
rlogin	Logs in to a UNIX host using rlogin.															
show hosts	Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses.															
show tcp	Displays the status of TCP connections.															
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<p>This command configures the HTTP server to request an X.509v3 certificate from the client in order to authenticate the client during the connection process.</p> <p>In the default connection and authentication process, the client requests a certificate from the HTTP server, but the server does not attempt to authenticate the client. Authenticating the client provides more security than server authentication by itself, but not all web clients may be configured for certificate authority (CA) authentication.</p> Cisco IOS HTTP Services Configuration Guide at 47 (2011).	Examples <ul style="list-style-type: none">These commands configures the HTTP server to request an X.509 certificate from the client in order to authenticate the client during the connection process. <pre>switch(config)#management api http-commands switch(config-mgmt-api-http-cmds)#protocol https certificate switch(config-mgmt-api-http-cmds)#</pre> Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 87. <i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 75.														

Copyright Registration Information	Cisco	Arista				
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<table><tr><td><i>start-ip</i></td><td>Starting IP address that defines the range of addresses in the address pool.</td></tr><tr><td><i>end-ip</i></td><td>Ending IP address that defines the range of addresses in the address pool.</td></tr></table> Cisco IOS IP Addressing Services Command Reference at 22 (2011).	<i>start-ip</i>	Starting IP address that defines the range of addresses in the address pool.	<i>end-ip</i>	Ending IP address that defines the range of addresses in the address pool.	<i>start_addr</i> The starting IP address that defines the range of addresses in the address pool (IPv4 addresses in dotted decimal notation). <i>end_addr</i> The ending IP address that defines the range of addresses in the address pool. (IPv4 addresses in dotted decimal notation). Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1278. <i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1075.
<i>start-ip</i>	Starting IP address that defines the range of addresses in the address pool.					
<i>end-ip</i>	Ending IP address that defines the range of addresses in the address pool.					
Cisco IOS 15.4 Effective date of registration: 11/26/2014	clear arp-cache To refresh dynamically created entries from the Address Resolution Protocol (ARP) cache, use the clear arp-cache command in privileged EXEC mode. clear arp-cache [interface type number] [vrf vrf-name] ip-address Cisco IOS IP Addressing Services Command Reference at 59 (2011).	clear arp-cache The clear arp-cache command refreshes dynamic entries in the Address Resolution Protocol (ARP) cache. Refreshing the ARP cache updates IP address and MAC address mapping information in the ARP table and removes expired ARP entries not yet deleted by an internal, timer-driven process. The command, without arguments, refreshes ARP cache entries for all enabled interfaces. With arguments, the command refreshes cache entries for the specified interface. Executing clear arp-cache for all interfaces can result in extremely high CPU usage while the tables are resolving. Platform all Command Mode Privileged EXEC Command Syntax clear arp-cache [VRF_INSTANCE] [INTERFACE_NAME] Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1255. <i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1060; Arista User Manual, v. 4.11.1 (1/11/13), at 846; Arista User Manual v. 4.10.3 (10/22/12), at 692.				

Copyright Registration Information	Cisco	Arista				
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<div><div>ip address</div><div>To set a primary or secondary IP address for an interface, use the ip address command in interface configuration mode. To remove an IP address or disable IP processing, use the no form of this command.</div><div><div>ip address ip-address mask [secondary [vrf vrf-name]]</div><div>no ip address ip-address mask [secondary [vrf vrf-name]]</div></div><div>Cisco IOS IP Addressing Services Command Reference at 166 (2011)</div><div><div>An interface can have one primary IP address and multiple secondary IP addresses</div><div>Packets generated by the Cisco IOS software always use the primary IP address. Therefore, all routers and access servers on a segment should share the same primary network number.</div><div>Hosts can determine subnet masks using the Internet Control Message Protocol (ICMP) mask request message. Routers respond to this request with an ICMP mask reply message.</div><div>You can disable IP processing on a particular interface by removing its IP address with the no ip address command. If the software detects another host using one of its IP addresses, it will print an error message on the console.</div><div>The optional secondary keyword allows you to specify an unlimited number of secondary addresses. Secondary addresses are treated like primary addresses, except the system never generates datagrams other than routing updates with secondary source addresses. IP broadcasts and Address Resolution Protocol (ARP) requests are handled properly, as are interface routes in the IP routing table.</div></div><div>Cisco IOS IP Addressing Services Command Reference at 167 (2011).</div></div>	<div><div>Ip address</div><div>The ip address command configures the IPv4 address and connected subnet on the configuration mode interface. Each interface can have one primary address and multiple secondary addresses.</div><div>The no ip address and default ip address commands remove the IPv4 address assignment from the configuration mode interface. Entering the command without specifying an address removes the primary and all secondary addresses from the interface. The primary address cannot be deleted until all secondary addresses are removed from the interface.</div><div>Removing all IPv4 address assignments from an interface disables IPv4 processing on that port.</div><div><table><tr><td>Platform</td><td>all</td></tr><tr><td>Command Mode</td><td>Interface-Ethernet Configuration Interface-Loopback Configuration Interface-Management Configuration Interface-Port-channel Configuration Interface-VLAN Configuration</td></tr></table></div><div><div>Command Syntax</div><div><div>ip address ipv4_subnet [PRIORITY]</div><div>no ip address [ipv4_subnet] [PRIORITY]</div><div>default ip address [ipv4_subnet] [PRIORITY]</div></div></div><div>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1262.</div><div>See also Arista User Manual v. 4.12.3 (7/17/13), at 1066; Arista User Manual, v. 4.11.1 (1/11/13), at 850; Arista User Manual v. 4.10.3 (10/22/12), at 696.</div></div>	Platform	all	Command Mode	Interface-Ethernet Configuration Interface-Loopback Configuration Interface-Management Configuration Interface-Port-channel Configuration Interface-VLAN Configuration
	Platform	all				
	Command Mode	Interface-Ethernet Configuration Interface-Loopback Configuration Interface-Management Configuration Interface-Port-channel Configuration Interface-VLAN Configuration				

Copyright Registration Information	Cisco	Arista									
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<p>ip nat inside destination</p> <p>To enable the Network Address Translation (NAT) of a globally unique outside host address to multiple inside host addresses, use the ip nat inside destination command in global configuration mode. This command is primarily used to implement TCP load balancing by performing destination address rotary translation. To remove the dynamic association to a pool, use the no form of this command.</p> <pre>ip nat inside destination list {access-list-number name} pool name [mapping-id map-id] no ip nat inside destination list {access-list-number name} pool name [mapping-id map-id]</pre> <table border="1"> <tr> <td data-bbox="306 505 426 521">Syntax Description</td><td data-bbox="449 505 762 521">list access-list-number</td><td data-bbox="772 505 1073 581">Standard IP access list number. Packets with destination addresses that pass the access list are translated using global addresses from the named pool.</td></tr> <tr> <td></td><td data-bbox="449 597 510 613">list name</td><td data-bbox="772 597 1073 673">Name of a standard IP access list. Packets with destination addresses that pass the access list are translated using global addresses from the named pool.</td></tr> <tr> <td></td><td data-bbox="449 683 520 699">pool name</td><td data-bbox="772 683 1073 716">Name of the pool from which global IP addresses are allocated during dynamic translation.</td></tr> </table> <p>Cisco IOS IP Addressing Services Command Reference at 405 (2011).</p>	Syntax Description	list access-list-number	Standard IP access list number. Packets with destination addresses that pass the access list are translated using global addresses from the named pool.		list name	Name of a standard IP access list. Packets with destination addresses that pass the access list are translated using global addresses from the named pool.		pool name	Name of the pool from which global IP addresses are allocated during dynamic translation.	<p>ip nat pool</p> <p>The ip nat pool command defines a pool of addresses using start address, end address, and either netmask or prefix length. If its starting IP address and ending IP address are the same, there is only one address in the address pool.</p> <p>During address translation, the NAT server selects an IP address from the address pool to be the translated source address.</p> <p>The no ip nat pool removes the corresponding ip nat pool command from <i>running-config</i>.</p> <p>Platform FM6000 Command Mode Global Configuration</p> <p>Command Syntax</p> <pre>ip nat pool pool_name [ADDRESS_SPAN] SUBNET_SIZE no ip nat pool pool_name default ip nat pool pool_name</pre> <p>Parameters</p> <ul style="list-style-type: none"> pool_name name of the pool from which global IP addresses are allocated. <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1278.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1075.</p>
Syntax Description	list access-list-number	Standard IP access list number. Packets with destination addresses that pass the access list are translated using global addresses from the named pool.									
	list name	Name of a standard IP access list. Packets with destination addresses that pass the access list are translated using global addresses from the named pool.									
	pool name	Name of the pool from which global IP addresses are allocated during dynamic translation.									

Copyright Registration Information	Cisco	Arista				
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<div>ip nat source</div> <p>To enable Network Address Translation (NAT) on a virtual interface without inside or outside specification, use the ip nat source command in global configuration mode.</p> <p>Cisco IOS IP Addressing Services Command Reference (2011), at 439.</p> <table><tr><td>pool name</td><td>Name of the pool from which global IP addresses are allocated dynamically.</td></tr><tr><td>overload</td><td>(Optional) Enables the router to use one global address for many local addresses. When overloading is configured, the TCP or User Datagram Protocol (UDP) port number of each inside host distinguishes between the multiple conversations using the same local IP address.</td></tr></table> <p>Cisco IOS IP Addressing Services Command Reference (2011), at 440.</p>	pool name	Name of the pool from which global IP addresses are allocated dynamically.	overload	(Optional) Enables the router to use one global address for many local addresses. When overloading is configured, the TCP or User Datagram Protocol (UDP) port number of each inside host distinguishes between the multiple conversations using the same local IP address.	<div>ip nat source dynamic</div> <p>The ip nat source dynamic command enables Network Address Translation (NAT) of a specified source address for packets sent and received on the configuration mode interface. This command installs hardware translation entries for forward and reverse traffic. When the rule specifies a group, the command does not install the reverse path in hardware. The command may include an access control list to filter packets for translation.</p> <p>...</p> <div>overload</div> <p>Enables the switch to use one global address for many local addresses. When overloading is configured, the TCP or User Datagram Protocol (UDP) port number of each inside host distinguishes between the multiple conversations using the same local IP address.</p> <div>pool pool_name</div> <p>The name of the pool from which global IP addresses are allocated dynamically.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/14), at 1279.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1076.</p>
	pool name	Name of the pool from which global IP addresses are allocated dynamically.				
	overload	(Optional) Enables the router to use one global address for many local addresses. When overloading is configured, the TCP or User Datagram Protocol (UDP) port number of each inside host distinguishes between the multiple conversations using the same local IP address.				

Copyright Registration Information	Cisco	Arista																
<div>Copyright Registration Information</div> <div>Cisco IOS 15.4</div> <div>Effective date of registration: 11/26/2014</div>	<div><div>ip nat pool</div><div>To define a pool of IP addresses for Network Address Translation (NAT), use the <code>ip nat pool</code> command in global configuration mode. To remove one or more addresses from the pool, use the <code>no</code> form of this command.</div><div><div><code>ip nat pool</code> <i>name</i> <i>start-ip</i> <i>end-ip</i> [<i>netmask netmask</i> <i>prefix-length prefix-length</i>] [<i>add-route</i>] [<i>type {match-host rotary}</i>] [<i>accounting list-name</i>] [<i>arp-ping</i>] [<i>noreservation</i>]</div><div><code>no ip nat pool</code> <i>name</i> <i>start-ip</i> <i>end-ip</i> [<i>netmask netmask</i> <i>prefix-length prefix-length</i>] [<i>add-route</i>] [<i>type {match-host rotary}</i>] [<i>accounting list-name</i>] [<i>arp-ping</i>] [<i>noreservation</i>]</div></div><div><table><tr><th>Syntax Description</th><th></th></tr><tr><td><i>name</i></td><td>Name of the pool.</td></tr><tr><td><i>start-ip</i></td><td>Starting IP address that defines the range of addresses in the address pool.</td></tr><tr><td><i>end-ip</i></td><td>Ending IP address that defines the range of addresses in the address pool.</td></tr><tr><td><i>netmask netmask</i></td><td>Specifies the network mask that indicates which address bits belong to the network and subnetwork fields and which bits belong to the host field. Specify the netmask of the network to which the pool addresses belong.</td></tr><tr><td><i>prefix-length prefix-length</i></td><td>Specifies the number that indicates how many bits of the netmask are ones (how many bits of the address indicate network). Specify the netmask of the network to which the pool addresses belong.</td></tr></table></div><div>Cisco IOS IP Addressing Services Command Reference (2011), at 422.</div><div><div>This command defines a pool of addresses using start address, end address, and either netmask or prefix length. The pool could define an inside global pool, an outside local pool, or a rotary pool.</div></div><div>Cisco IOS IP Addressing Services Command Reference (2011), at 423.</div></div>	Syntax Description		<i>name</i>	Name of the pool.	<i>start-ip</i>	Starting IP address that defines the range of addresses in the address pool.	<i>end-ip</i>	Ending IP address that defines the range of addresses in the address pool.	<i>netmask netmask</i>	Specifies the network mask that indicates which address bits belong to the network and subnetwork fields and which bits belong to the host field. Specify the netmask of the network to which the pool addresses belong.	<i>prefix-length prefix-length</i>	Specifies the number that indicates how many bits of the netmask are ones (how many bits of the address indicate network). Specify the netmask of the network to which the pool addresses belong.	<div><div>ip nat pool</div><div>The <code>ip nat pool</code> command defines a pool of addresses using start address, end address, and either netmask or prefix length. If its starting IP address and ending IP address are the same, there is only one address in the address pool.</div><div>During address translation, the NAT server selects an IP address from the address pool to be the translated source address.</div><div>The <code>no ip nat pool</code> removes the corresponding <code>ip nat pool</code> command from <i>running_config</i>.</div><div><table><tr><td>Platform</td><td>FM6000</td></tr><tr><td>Command Mode</td><td>Global Configuration</td></tr></table></div><div>Command Syntax</div><div><div><code>ip nat pool</code> <i>pool_name</i> [<i>ADDRESS_SPAN</i>] <i>SUBNET_SIZE</i></div><div><code>no ip nat pool</code> <i>pool_name</i></div><div><code>default ip nat pool</code> <i>pool_name</i></div></div><div>Parameters</div><div><ul style="list-style-type: none"><i>pool_name</i> name of the pool from which global IP addresses are allocated.<i>ADDRESS_SPAN</i> Options include:<ul style="list-style-type: none"><i>start_addr</i> The starting IP address that defines the range of addresses in the address pool (IPv4 addresses in dotted decimal notation).<i>end_addr</i> The ending IP address that defines the range of addresses in the address pool. (IPv4 addresses in dotted decimal notation).<i>SUBNET_SIZE</i> this functions as a sanity check to ensure it is not a network or broadcast network. Options include:<ul style="list-style-type: none"><i>netmask ipv4_addr</i> The network mask that indicates which address bits belong to the network and subnetwork fields and which bits belong to the host field. Specify the netmask of the network to which the pool addresses belong (dotted decimal notation).<i>prefix-length <0 to 32></i> The number that indicates how many bits of the netmask are ones (how many bits of the address indicate network). Specify the netmask of the network to which the pool addresses belong.</div><div>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1278.</div><div>See also Arista User Manual v. 4.12.3 (7/17/13), at 1075.</div></div>	Platform	FM6000	Command Mode	Global Configuration
	Syntax Description																	
	<i>name</i>	Name of the pool.																
	<i>start-ip</i>	Starting IP address that defines the range of addresses in the address pool.																
	<i>end-ip</i>	Ending IP address that defines the range of addresses in the address pool.																
<i>netmask netmask</i>	Specifies the network mask that indicates which address bits belong to the network and subnetwork fields and which bits belong to the host field. Specify the netmask of the network to which the pool addresses belong.																	
<i>prefix-length prefix-length</i>	Specifies the number that indicates how many bits of the netmask are ones (how many bits of the address indicate network). Specify the netmask of the network to which the pool addresses belong.																	
Platform	FM6000																	
Command Mode	Global Configuration																	

Copyright Registration Information	Cisco	Arista				
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<p>ip nat translation (timeout)</p> <p>To change the amount of time after which Network Address Translation (NAT) translations time out, use the ip nat translation command in global configuration mode. To disable the timeout, use the no form of this command.</p> <p>ip nat translation {arp-ping-timeout dns-timeout first-timeout icmp-timeout port-timeout {tcp port-number udp port-number} pptp-timeout routemap-entry-timeout syn-timeout tcp-timeout timeout udp-timeout} [seconds never]</p> <p>Cisco IOS IP Addressing Services Command Reference (2011), at 446.</p> <table><tr><td><i>seconds</i></td><td>Number of seconds after which the specified port translation times out.</td></tr></table> <p>Cisco IOS IP Addressing Services Command Reference (2011), at 447.</p>	<i>seconds</i>	Number of seconds after which the specified port translation times out.	<p>Use the ip nat translation tcp-timeout or ip nat translation udp-timeout commands to change the amount of time after which Network Address Translation (NAT) translations time out.</p> <p>Example</p> <ul style="list-style-type: none">This command globally sets the inactive timeout for TCP to 600 seconds. switch(config)# ip nat translation tcp-timeout 600 switch(config)#This command globally sets the inactive timeout for UDP to 800 seconds. switch#(config)# ip nat translation udp-timeout 800 switch#(config)# <p>Arista User Manual 4.14.3F (Rev. 2) (10/2/2014), at 1247</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1053.</p> <p><i>period</i> The number of seconds after which the specified port translation times out. Value ranges from 0 to 4294967295. Default value is 86400 (24 hours).</p> <p>Arista User Manual 4.14.3F (Rev. 2) (10/2/2014), at 1284</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1079.</p>		
	<i>seconds</i>	Number of seconds after which the specified port translation times out.				
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<table><tr><th>Command</th><th>Description</th></tr><tr><td>show ip dhcp snooping</td><td>Displays the DHCP snooping configuration.</td></tr></table> <p>Cisco IOS IP Addressing Services Command Reference (2011), at 311.</p>	Command	Description	show ip dhcp snooping	Displays the DHCP snooping configuration.	<p>show ip dhcp snooping</p> <p>The show ip dhcp snooping command displays the DHCP snooping configuration.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1302.</p>
Command	Description					
show ip dhcp snooping	Displays the DHCP snooping configuration.					

Copyright Registration Information	Cisco	Arista								
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<div>show ip dhcp snooping</div> <div>To display the DHCP snooping configuration, use the <code>show ip dhcp snooping</code> command in privileged EXEC mode.</div> <div>show ip dhcp snooping</div> <div>...</div> <table><thead><tr><th>Command</th><th>Description</th></tr></thead><tbody><tr><td>ip dhcp snooping</td><td>Globally enables DHCP snooping.</td></tr><tr><td>ip dhcp snooping binding</td><td>Sets up and generates a DHCP binding configuration to restore bindings across reboots.</td></tr></tbody></table> <div>Cisco IOS IP Addressing Services Command Reference (2011), at 673.</div> <table><tbody><tr><td>ip dhcp snooping vlan</td><td>Enables DHCP snooping on a VLAN or a group of VLANs.</td></tr></tbody></table> <div>Cisco IOS IP Addressing Services Command Reference (2011), at 674.</div>	Command	Description	ip dhcp snooping	Globally enables DHCP snooping.	ip dhcp snooping binding	Sets up and generates a DHCP binding configuration to restore bindings across reboots.	ip dhcp snooping vlan	Enables DHCP snooping on a VLAN or a group of VLANs.	<div>show ip dhcp snooping</div> <div>The <code>show ip dhcp snooping</code> command displays the DHCP snooping configuration.</div> <div>Platform Trident Command Mode EXEC</div> <div>Command Syntax</div> <div>show ip dhcp snooping</div> <div>Related Commands</div> <ul style="list-style-type: none"><code>ip dhcp snooping</code> globally enables DHCP snooping.<code>ip dhcp snooping vlan</code> enables DHCP snooping on specified VLANs<code>ip dhcp snooping information option</code> enables insertion of option-82 snooping data.<code>ip helper-address</code> enables the DHCP relay agent on a configuration mode interface. <div>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1302.</div>
	Command	Description								
ip dhcp snooping	Globally enables DHCP snooping.									
ip dhcp snooping binding	Sets up and generates a DHCP binding configuration to restore bindings across reboots.									
ip dhcp snooping vlan	Enables DHCP snooping on a VLAN or a group of VLANs.									
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<table><thead><tr><th>Command</th><th>Description</th></tr></thead><tbody><tr><td>dir</td><td>Displays a list of files on a file system.</td></tr></tbody></table> <div>Cisco IOS IP Application Services Command Reference (2013), at 283.</div>	Command	Description	dir	Displays a list of files on a file system.	<div>dir</div> <div>The <code>dir</code> command displays a list of files on a file system.</div> <div>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 139</div> <div>Arista User Manual v. 4.12.3 (7/17/13), at 115; Arista User Manual, v. 4.11.1 (1/11/13), at 55.</div>				
Command	Description									
dir	Displays a list of files on a file system.									

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<div data-bbox="306 280 1115 329"> <code>show ip mroute</code> Displays the contents of the IP multicast routing table. </div> <p>Cisco IOS IP Switching Command Reference (2013), at 483.</p>	<div data-bbox="1178 280 2032 313"> The <code>show ip mroute</code> command displays the contents of the IP multicast routing table. </div> <ul style="list-style-type: none"> <code>show ip mroute</code> displays information for all routes in the table. <code>show ip mroute gp_addr</code> displays information for the specified multicast group. <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1757</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1485; Arista User Manual, v. 4.11.1 (1/11/13), at 1187; Arista User Manual v. 4.10.3 (10/22/12), at 1022; Arista User Manual v. 4.9.3.2 (5/3/12), at 780; Arista User Manual v. 4.8.2 (11/18/11), at 599.</p>
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<div data-bbox="306 664 1115 922"> <code>community-string</code> <div data-bbox="709 672 1104 721"> Password-like community string sent with the notification operation. </div> <div data-bbox="709 729 1104 867"> Note You can set this string using the <code>snmp-server host</code> command by itself, but Cisco recommends that you define the string using the <code>snmp-server community</code> command prior to using the <code>snmp-server host</code> command. </div> <div data-bbox="709 867 1104 915"> Note The "at" sign (@) is used for delimiting the context information. </div> </div> <p>Cisco IOS IP Switching Command Reference (2013), at 526.</p>	<ul style="list-style-type: none"> <code>comm_str</code> community string (used as password) sent with the notification operation. <div data-bbox="1199 696 2032 745"> Although this string can be set with the <code>snmp-server host</code> command, the preferred method is defining it with the <code>snmp-server community</code> command prior to using this command. </div> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1995.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1685; Arista User Manual, v. 4.11.1 (1/11/13), at 1370; Arista User Manual v. 4.10.3 (10/22/12), at 1137; Arista User Manual v. 4.9.3.2 (5/3/12), at 893; Arista User Manual v. 4.8.2 (11/18/11), at 700; Arista User Manual v. 4.7.3 (7/18/11), at 479.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<p>SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response protocol data unit (PDU). If the sender never receives the response, the inform request can be sent again. Thus, informs are more likely to reach their intended destination than traps.</p> <p>Compared to traps, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Also, traps are sent only once; an inform may be tried several times. The retries increase traffic and contribute to a higher overhead on the network.</p> <p>Cisco IOS IP Switching Command Reference (2013), at 530.</p>	<p>37.2.2 SNMP Notifications</p> <p>SNMP notifications are messages, sent by the agent, to inform managers of an event or a network condition. A <i>trap</i> is an unsolicited notification. An <i>inform</i> (or inform request) is a trap that includes a request for a confirmation that the message is received. Events that a notification can indicate include improper user authentication, restart, and connection losses.</p> <p>Traps are less reliable than informs because the receiver does not send any acknowledgment. However, traps are often preferred because informs consume more switch and network resources. A trap is sent only once and is discarded as soon as it is sent. An inform request remains in memory until a response is received or the request times out. An inform may be retried several times, increasing traffic and contributing to higher network overhead.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1963,</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 1891; Arista User Manual v. 4.12.3 (7/17/13), at 1653; Arista User Manual, v. 4.11.1 (1/11/13), at 1341; Arista User Manual v. 4.10.3 (10/22/12), at 1107; Arista User Manual v. 4.9.3.2 (5/3/12), at 863; Arista User Manual v. 4.8.2 (11/18/11), at 675; Arista User Manual v. 4.7.3 (7/18/11), at 531.</p>
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<p>nssa-only</p> <p>(Optional) Limits the default advertisement to this NSSA area by setting the propagate (P) bit in the type-7 LSA to zero.</p> <p>Cisco IOS IP Routing:OSPF Command Reference (2013), at 9.</p>	<p>TYPE area type. Values include:</p> <ul style="list-style-type: none"> <no parameter> area is configured as a not-so-stubby area (NSSA). nssa-only limits the default advertisement to this NSSA area by setting the propagate (P) bit in the type-7 LSA to zero. <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/14), at 1498.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1283; Arista User Manual, v. 4.11.1 (1/11/13), at 958.</p>

Copyright Registration Information	Cisco	Arista										
	<div><div>area nssa translate</div><div><p>To configure a not-so-stubby area (NSSA) and to configure the OSPF Forwarding Address Suppression in Translated Type-5 LSAs feature, use the <code>area nssa translate</code> command in router address family topology or router configuration mode. To remove the NSSA distinction from the area, use the <code>no</code> form of this command.</p><div><div>area nssa translate</div><div>ommandarea <i>area-id</i> nssa translate type7 [<i>always</i>] [<i>suppress-fa</i>] [<i>default-information-originate</i> [<i>metric</i> <i>ospf-metric</i>] [<i>metric-type</i> <i>ospf-link-state-type</i>] [<i>nssa-only</i>] [<i>no-ext-capability</i>] [<i>no-redistribution</i>] [<i>no-summary</i>]</div></div><div><div>no area <i>area-id</i> nssa translate type7 [<i>always</i>] [<i>suppress-fa</i>] [<i>default-information-originate</i> [<i>metric</i> <i>ospf-metric</i>] [<i>metric-type</i> <i>ospf-link-state-type</i>] [<i>nssa-only</i>] [<i>no-ext-capability</i>] [<i>no-redistribution</i>] [<i>no-summary</i>]</div></div><div><table><tr><th>Syntax Description</th><th></th></tr><tr><td><i>area-id</i></td><td>Identifier for the stub area or NSSA. The identifier can be specified as either a decimal value or an IP address.</td></tr><tr><td>translate</td><td>Translates one type of link-state advertisement (LSA) to another type of LSA. This keyword takes effect only on an NSSA Area Border Router (ABR) or an NSSA Autonomous System Boundary Router (ASBR).</td></tr><tr><td>type7</td><td>(Required) Translates a Type-7 LSA to a Type-5 LSA. This keyword takes effect only on an NSSA ABR or an NSSA ASBR.</td></tr><tr><td>always</td><td>(Optional) Configures an NSSA ABR router as a forced NSSA LSA translator. The NSSA ABR router unconditionally translates Type-7 LSAs to Type-5 LSAs. You can configure the <code>always</code> keyword only in router configuration mode, not in router address family topology configuration mode.</td></tr></table></div></div></div> <div><div>Cisco IOS 15.4</div><div>Effective date of registration: 11/26/2014</div></div> <div>Cisco IOS IP Routing:OSPF Command Reference (2013), at 11.</div>	Syntax Description		<i>area-id</i>	Identifier for the stub area or NSSA. The identifier can be specified as either a decimal value or an IP address.	translate	Translates one type of link-state advertisement (LSA) to another type of LSA. This keyword takes effect only on an NSSA Area Border Router (ABR) or an NSSA Autonomous System Boundary Router (ASBR).	type7	(Required) Translates a Type-7 LSA to a Type-5 LSA. This keyword takes effect only on an NSSA ABR or an NSSA ASBR.	always	(Optional) Configures an NSSA ABR router as a forced NSSA LSA translator. The NSSA ABR router unconditionally translates Type-7 LSAs to Type-5 LSAs. You can configure the <code>always</code> keyword only in router configuration mode, not in router address family topology configuration mode.	<div><div>area nssa translate type7 always (OSPFv3)</div><div><p>The <code>area nssa translate type7 always</code> command translates Type-7 link-state advertisement (LSA) to Type-5 of LSAs.</p><p>The <code>no area nssa translate type7 always</code> command removes the NSSA distinction from the area.</p><div><div>Platform</div><div>all</div></div><div><div>Command Mode</div><div>Router-OSPF3 Configuration</div></div><div><div>Command Syntax</div><div><div>area <i>area_id</i> nssa translate type7 always</div><div>no <i>area_id</i> nssa translate type7 always</div><div>default <i>area_id</i> nssa translate type7 always</div></div></div><div><div>Parameters</div><div><ul style="list-style-type: none"><i>area_id</i> area number<div><div>Valid formats: integer <1 to 4294967295> or dotted decimal <0.0.0.1 to 255.255.255.255></div><div>Area 0 (or 0.0.0.0) is not configurable; it is always <i>normal</i>.</div><div><i>Running-config</i> stores value in dotted decimal notation.</div></div></div><div><div>Example</div><div><ul style="list-style-type: none">This command configures an NSSA ABR router as a forced NSSA LSA translator. The NSSA ABR router unconditionally translates Type-7 LSAs to Type-5 LSAs.</div></div></div><div><div>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1501.</div><div>See also Arista User Manual v. 4.13.6F (4/14/2014), at 1451; Arista User Manual v. 4.12.3 (7/17/13), at 1286; Arista User Manual, v. 4.11.1 (1/11/13), at 1036.</div></div></div></div>
Syntax Description												
<i>area-id</i>	Identifier for the stub area or NSSA. The identifier can be specified as either a decimal value or an IP address.											
translate	Translates one type of link-state advertisement (LSA) to another type of LSA. This keyword takes effect only on an NSSA Area Border Router (ABR) or an NSSA Autonomous System Boundary Router (ASBR).											
type7	(Required) Translates a Type-7 LSA to a Type-5 LSA. This keyword takes effect only on an NSSA ABR or an NSSA ASBR.											
always	(Optional) Configures an NSSA ABR router as a forced NSSA LSA translator. The NSSA ABR router unconditionally translates Type-7 LSAs to Type-5 LSAs. You can configure the <code>always</code> keyword only in router configuration mode, not in router address family topology configuration mode.											
	<div><table><tr><th>Command</th><th>Description</th></tr><tr><td>show ip route</td><td>Displays the current state of the routing table.</td></tr></table><div><div>Cisco IOS 15.4</div><div>Effective date of registration: 11/26/2014</div></div><div>Cisco IOS IP Routing:OSPF Command Reference (2013), at 51.</div></div>	Command	Description	show ip route	Displays the current state of the routing table.	<div><div>show ip route age</div><div><p>The <code>show ip route age</code> command displays the current state of the routing table and specifies the time the route was updated.</p></div><div><div>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1313.</div><div>See also Arista User Manual v. 4.12.3 (7/17/13), at 1102.</div></div></div>						
Command	Description											
show ip route	Displays the current state of the routing table.											

Copyright Registration Information	Cisco	Arista												
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<div>ip ospf name-lookup</div> <p>To configure Open Shortest Path First (OSPF) to look up Domain Name System (DNS) names for use in all OSPF <code>show EXEC</code> command displays, use the <code>ip ospf name-lookup</code> command in global configuration mode. To disable this function, use the <code>no</code> form of this command.</p> <div>ip ospf name-lookup no ip ospf name-lookup</div> <p>Syntax Description This command has no arguments or keywords.</p> <p>Command Default This command is disabled by default.</p> <p>Command Modes Global configuration</p> <table><tr><th>Release</th><th>Modification</th></tr><tr><td>10.0</td><td>This command was introduced.</td></tr><tr><td>12.2(33)SRA</td><td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td></tr><tr><td>12.2SX</td><td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td></tr></table> <p>Usage Guidelines This command makes it easier to identify a router because the router is displayed by name rather than by its router ID or neighbor ID.</p> <p>Cisco IOS IP Routing:OSPF Command Reference (2013), at 109.</p>	Release	Modification	10.0	This command was introduced.	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.	<div>ip ospf name-lookup</div> <p>The <code>ip ospf name-lookup</code> command causes the switch to display DNS names in place of numeric OSPFv2 router IDs in all subsequent OSPFv2 show commands, including:</p> <ul style="list-style-type: none"><code>show ip ospf</code><code>show ip ospf border-routers</code><code>show ip ospf database <link state list></code><code>show ip ospf database database-summary</code><code>show ip ospf database <link-state details></code><code>show ip ospf interface</code><code>show ip ospf neighbor</code><code>show ip ospf request-list</code><code>show ip ospf retransmission-list</code> <p>Although this command makes it easier to identify a router, the switch relies on a configured DNS server to respond to reverse DNS queries, which may be slower than displaying numeric router IDs.</p> <p>The <code>no ip ospf name-lookup</code> and default <code>ip ospf name-lookup</code> commands remove the <code>ip ospf name-lookup</code> command from <i>running-config</i>, restoring the default behavior of displaying OSPFv2 router IDs by their numeric value.</p> <table><tr><td>Platform</td><td>all</td></tr><tr><td>Command Mode</td><td>Global Configuration</td></tr></table> <p>Command Syntax</p> <div>ip ospf name-lookup no ip ospf name-lookup default ip ospf name-lookup</div> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1431.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1218; Arista User Manual, v. 4.11.1 (1/11/13), at 975; Arista User Manual v. 4.10.3 (10/22/12), at 805; Arista User Manual v. 4.9.3.2 (5/3/12), at 628; Arista User Manual v. 4.8.2 (11/18/11), at 464; Arista User Manual v. 4.7.3 (7/18/11), at 337; Arista User Manual v. 4.6.0 (12/22/2010), at 200.</p>	Platform	all	Command Mode	Global Configuration
	Release	Modification												
	10.0	This command was introduced.												
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.													
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.													
Platform	all													
Command Mode	Global Configuration													

Copyright Registration Information	Cisco	Arista			
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<p>log-adjacency-changes</p> <p>To configure the router to send a syslog message when an Open Shortest Path First (OSPF) neighbor goes up or down, use the log-adjacency-changes command in router configuration mode. To turn off this function, use the no form of this command.</p> <p>log-adjacency-changes [detail] no log-adjacency-changes [detail]</p> <table border="1"> <tr> <td>Syntax Description</td><td>detail</td><td>(Optional) Sends a syslog message for each state change, not just when a neighbor goes up or down.</td></tr> </table> <p>Cisco IOS IP Routing:OSPF Command Reference (2013), at 131.</p>	Syntax Description	detail	(Optional) Sends a syslog message for each state change, not just when a neighbor goes up or down.	<p>log-adjacency-changes (OSPFv3)</p> <p>The log-adjacency-changes command configures the switch to send syslog messages when it detects a neighbor has gone up or down. Log message sending is disabled by default. Valid options include:</p> <ul style="list-style-type: none"> log-adjacency-changes: switch sends syslog messages when a neighbor goes up or down (default). no log-adjacency-changes disables link state change syslog reporting. <p>The default option is active when <i>running-config</i> does not contain any form of the command. Entering the command in any form replaces the previous command state in <i>running-config</i>. The default log-adjacency-changes command restores the default state by removing the log-adjacency-changes statement from <i>running-config</i>.</p> <p>Platform all Command Mode Router-OSPF3 Configuration</p> <p>Command Syntax</p> <p>log-adjacency-changes [INFO_LEVEL] no log-adjacency-changes default log-adjacency-changes</p> <p>Parameters</p> <ul style="list-style-type: none"> INFO_LEVEL specifies the type of information displayed. Options include <ul style="list-style-type: none"> <no parameter> displays all log adjacency change messages detail displays syslog message for each state change, not just when a neighbor goes up or down. <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1518.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1303; Arista User Manual, v. 4.11.1 (1/11/13), at 1054; Arista User Manual v. 4.10.3 (10/22/12), at 811.</p>
Syntax Description	detail	(Optional) Sends a syslog message for each state change, not just when a neighbor goes up or down.			

Copyright Registration Information	Cisco	Arista														
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<div>max-metric router-lsa</div> <div>To configure a router that is running the Open Shortest Path First (OSPF) protocol to advertise a maximum metric so that other routers do not prefer the router as an intermediate hop in their shortest path first (SPF) calculations, use the max-metric router-lsa command in router address family topology or router configuration mode. To disable the advertisement of a maximum metric, use the no form of this command.</div> <div>max-metric router-lsa [external-lsa [max-metric-value]] [include-stub] [on-startup {seconds} wait-for-bgp] [summary-lsa [max-metric-value]] no max-metric router-lsa [external-lsa [max-metric-value]] [include-stub] [on-startup {seconds} wait-for-bgp] [summary-lsa [max-metric-value]]</div> <div><div>Syntax Description</div><table><tr><td>external-lsa</td><td>(Optional) Configures the router to override the external LSA metric with the maximum metric value.</td></tr><tr><td>max-metric-value</td><td>(Optional) Maximum metric value for LSAs. The configurable range is from 1 to 16777215. The default value is 16711680.</td></tr><tr><td>include-stub</td><td>(Optional) Configures the router to advertise the maximum metric for stub links in router LSAs.</td></tr><tr><td>on-startup</td><td>(Optional) Configures the router to advertise a maximum metric at startup.</td></tr><tr><td>seconds</td><td>(Optional) Maximum metric value for the specified time interval. The configurable range is from 5 to 86400 seconds. There is no default timer value for this configuration option.</td></tr><tr><td>wait-for-bgp</td><td>(Optional) Configures the router to advertise a maximum metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired. The default timer is 600 seconds.</td></tr><tr><td>summary-lsa</td><td>(Optional) Configures the router to override the summary LSA metric with the maximum metric value.</td></tr></table></div> <div>Cisco IOS IP Routing:OSPF Command Reference (2013), at 136.</div>	external-lsa	(Optional) Configures the router to override the external LSA metric with the maximum metric value.	max-metric-value	(Optional) Maximum metric value for LSAs. The configurable range is from 1 to 16777215. The default value is 16711680.	include-stub	(Optional) Configures the router to advertise the maximum metric for stub links in router LSAs.	on-startup	(Optional) Configures the router to advertise a maximum metric at startup.	seconds	(Optional) Maximum metric value for the specified time interval. The configurable range is from 5 to 86400 seconds. There is no default timer value for this configuration option.	wait-for-bgp	(Optional) Configures the router to advertise a maximum metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired. The default timer is 600 seconds.	summary-lsa	(Optional) Configures the router to override the summary LSA metric with the maximum metric value.	<div>max-metric router-lsa (OSPFv3)</div> <div>The max-metric router-lsa command allows the OSPFv3 protocol to advertise a maximum metric so that other routers do not prefer the router as an intermediate hop in their SPF calculations.</div> <div>The no max-metric router-lsa and default max-metric router-lsa commands disable the advertisement of a maximum metric.</div> <div>Platformall Command ModeRouter-OSPF3 Configuration</div> <div>Command Syntax<div>max-metric router-lsa [EXTERNAL] [STUB] [STARTUP] [SUMMARY] no max-metric router-lsa [EXTERNAL] [STUB] [STARTUP] [SUMMARY] default max-metric router-lsa [EXTERNAL] [STUB] [STARTUP] [SUMMARY]</div><div>All parameters can be placed in any order.</div><div>Parameters<ul style="list-style-type: none">EXTERNALadvertised metric value. Values include:<ul style="list-style-type: none"><no parameter>Metric is set to the default value of 1.external-lsaConfigures the router to override the External LSA /NSSA-External metric with the maximum metric value.external-lsa <1 to 16777215>The configurable range is from 1 to 0xFFFFFFFF. The default value is 0xFF0000. This range can be used with external LSA, summary LSA extensions to indicate the respective metric you want with the LSA.STUBadvertised metric type. Values include:<ul style="list-style-type: none"><no parameter>Metric type is set to the default value of 2.include-stubAdvertises stub links in router-LSA with the max-metric value (0xFFFF).STARTUPlimit scope of LSAs. Values include:<ul style="list-style-type: none"><no parameter>LSA can be translatedon-startupConfigures the router to advertise a maximum metric at startup (only valid in no and default command formats).on-startup wait-for-bgpConfigures the router to advertise a maximum metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired. The default timer is 600 seconds.on-startup <5 to 86400>Sets the maximum metric temporarily after a reboot to originate router-LSAs with the max-metric value.<div>wait-for-bgp or an on-start time value is not included in no and default commands.</div>SUMMARYadvertised metric value. Values include:<ul style="list-style-type: none"><no parameter>Metric is set to the default value of 1.summary-lsaConfigures the router to override the summary LSA metric with the maximum metric value for both type 3 and type 4 Summary LSAs.summary-lsa <1 to 16777215>Metric is set to the specified value.</div><div>Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1519.</div></div>
	external-lsa	(Optional) Configures the router to override the external LSA metric with the maximum metric value.														
	max-metric-value	(Optional) Maximum metric value for LSAs. The configurable range is from 1 to 16777215. The default value is 16711680.														
include-stub	(Optional) Configures the router to advertise the maximum metric for stub links in router LSAs.															
on-startup	(Optional) Configures the router to advertise a maximum metric at startup.															
seconds	(Optional) Maximum metric value for the specified time interval. The configurable range is from 5 to 86400 seconds. There is no default timer value for this configuration option.															
wait-for-bgp	(Optional) Configures the router to advertise a maximum metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired. The default timer is 600 seconds.															
summary-lsa	(Optional) Configures the router to override the summary LSA metric with the maximum metric value.															

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<p>The following is sample output from the <code>show ip ospf</code> command when entered without a specific OSPF process ID:</p> <pre> Router# show ip ospf Routing Process "ospf 201" with ID 10.0.0.1 and Domain ID 10.20.0.1 Supports only single IOS(1080) routes Supports opaque LSA SPF schedule delay 5 secs, Hold time between two SPFs 10 secs Minimum LSA interval 5 secs, Minimum LSA arrival 1 secs LSA group pacing timer 100 secs Interface flood pacing timer 35 msec Retransmission pacing timer 100 msec Number of external LSA 0, Checksum Sum 0x0 Number of opaque AS LSA 0, Checksum Sum 0x0 Number of DCbitless external and opaque AS LSA 0 Number of DoNotAge external and opaque AS LSA 0 Number of areas in this router is 2, 2 normal 0 stub 0 nssa External flood list length 0 Area BACKBONE(0) Number of interfaces in this area is 2 Area has message digest authentication SPF algorithm executed 4 times Area ranges are Number of LSA 4, Checksum Sum 0x29BEB Number of opaque link LSA 0, Checksum Sum 0x0 Number of DCbitless LSA 3 Number of indication LSA 0 Number of DoNotAge LSA 0 Flood list length 0 Area 172.16.26.0 Number of interfaces in this area is 0 Area has no authentication SPF algorithm executed 1 times Area ranges are 192.168.0.0/16 Passive Advertise Number of LSA 1, Checksum Sum 0x44FD Number of opaque link LSA 0, Checksum Sum 0x0 Number of DCbitless LSA 1 Number of indication LSA 1 Number of DoNotAge LSA 0 Flood list length 0 </pre> <p>Cisco IOS IP Routing:OSPF Command Reference (2013), at 174.</p>	<pre> switch#show ip ospf Routing Process "ospf 1" with ID 10.168.103.1 Supports opaque LSA Maximum number of LSA allowed 12000 Threshold for warning message 75% Ignore-time 5 minutes, reset-time 5 minutes Ignore-count allowed 5, current 0 It is an area border router Hold time between two consecutive SPFs 5000 msec SPF algorithm last executed 00:00:09 ago Minimum LSA interval 5 secs Minimum LSA arrival 1000 msec Number of external LSA 0, Checksum Sum 0x000000 Number of opaque AS LSA 0, Checksum Sum 0x000000 Number of LSA 27. Number of areas in this router is 3, 3 normal 0 stub 0 nssa Area BACKBONE(0.0.0.0) Number of interfaces in this area is 2 It is a normal area Area has no authentication SPF algorithm executed 153 times Number of LSA 8, Checksum Sum 0x03e13a Number of opaque link LSA 0, Checksum Sum 0x000000 Area 0.0.0.2 Number of interfaces in this area is 1 It is a normal area Area has no authentication SPF algorithm executed 153 times Number of LSA 11, Checksum Sum 0x054e57 Number of opaque link LSA 0, Checksum Sum 0x000000 Area 0.0.0.3 Number of interfaces in this area is 1 It is a normal area Area has no authentication SPF algorithm executed 5 times Number of LSA 6, Checksum Sum 0x02a401 Number of opaque link LSA 0, Checksum Sum 0x000000 </pre> <p>Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1391-1392.</p>

Copyright Registration Information	Cisco	Arista
		<i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1180; Arista User Manual, v. 4.11.1 (1/11/13), at 939; Arista User Manual v. 4.10.3 (10/22/12), at 775; Arista User Manual v. 4.9.3.2 (5/3/12), at 645; Arista User Manual v. 4.8.2 (11/18/11), at 480; Arista User Manual v. 4.7.3 (7/18/11), at 353; Arista User Manual v. 4.6.0 (12/22/2010), at 213.

Copyright Registration Information	Cisco	Arista		
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<div>show ip ospf database</div> <div>To display lists of information related to the Open Shortest Path First (OSPF) database for a specific router, use the show ip ospf database command in EXEC mode.</div> <div>show ip ospf [process-id area-id] database</div> <div>Cisco IOS IP Routing:OSPF Command Reference (2013), at 184</div> <table><tr><td>link-state-id</td><td><div>(Optional) Portion of the Internet environment that is being described by the advertisement. The value entered depends on the advertisement's LS type. It must be entered in the form of an IP address.</div><div>When the link state advertisement is describing a network, the link-state-id can take one of two forms:</div><div>The network's IP address (as in type 3 summary link advertisements and in autonomous system external link advertisements).</div><div>A derived address obtained from the link state ID. (Note that masking a network links advertisement's link state ID with the network's subnet mask yields the network's IP address.)</div><div>When the link state advertisement is describing a router, the link state ID is always the described router's OSPF router ID.</div><div>When an autonomous system external advertisement (LS Type = 5) is describing a default route, its link state ID is set to Default Destination (0.0.0.0).</div></td></tr></table> <div>Cisco IOS IP Routing:OSPF Command Reference (2013), at 185.</div>	link-state-id	<div>(Optional) Portion of the Internet environment that is being described by the advertisement. The value entered depends on the advertisement's LS type. It must be entered in the form of an IP address.</div> <div>When the link state advertisement is describing a network, the link-state-id can take one of two forms:</div> <div>The network's IP address (as in type 3 summary link advertisements and in autonomous system external link advertisements).</div> <div>A derived address obtained from the link state ID. (Note that masking a network links advertisement's link state ID with the network's subnet mask yields the network's IP address.)</div> <div>When the link state advertisement is describing a router, the link state ID is always the described router's OSPF router ID.</div> <div>When an autonomous system external advertisement (LS Type = 5) is describing a default route, its link state ID is set to Default Destination (0.0.0.0).</div>	<div>show ip ospf database <link-state details></div> <div>The show ip ospf database <link-state details> command displays details of the specified link state advertisements (LSAs). The switch can return link state data about a single area or for all areas on the switch.</div> <div>Platformall Command ModeEXEC</div> <div>Command Syntax</div> <div>show ip ospf [AREA] database LINKSTATE_TYPE linkstate_id [ROUTER] [VRF_INSTANCE]</div> <div>...</div> <div><div>linkstate_id</div><div>Network segment described by the LSA (dotted decimal notation).</div><div>Value depends on the LSA type.</div><div><div>When the LSA describes a network, the linkstate-id argument is one of the following:</div><div>The network IP address, as in Type 3 summary link advertisements and in autonomous system external link advertisements.</div><div>A derived address obtained from the link state ID. Masking a network links the advertisement link state ID with the network subnet mask yielding the network IP address.</div><div>When the LSA describes a router, the link state ID is the OSPFv2 router ID of the router.</div><div>When an autonomous system external advertisement (Type 5) describes a default route, its link state ID is set to the default destination (0.0.0.0).</div></div></div> <div>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1454.</div> <div>See also Arista User Manual v. 4.13.6F (4/14/2014), at 1404; Arista User Manual v. 4.12.3 (7/17/13), at 1240; Arista User Manual, v. 4.11.1 (1/11/13), at 996; Arista User Manual v. 4.10.3 (10/22/12), at 825; Arista User Manual v. 4.9.3.2 (5/3/12), at 647; Arista User Manual v. 4.8.2 (11/18/11), at 483; Arista User Manual v. 4.7.3 (7/18/11), at 357; Arista User Manual v. 4.6.0 (12/22/2010), at 217.</div>
	link-state-id	<div>(Optional) Portion of the Internet environment that is being described by the advertisement. The value entered depends on the advertisement's LS type. It must be entered in the form of an IP address.</div> <div>When the link state advertisement is describing a network, the link-state-id can take one of two forms:</div> <div>The network's IP address (as in type 3 summary link advertisements and in autonomous system external link advertisements).</div> <div>A derived address obtained from the link state ID. (Note that masking a network links advertisement's link state ID with the network's subnet mask yields the network's IP address.)</div> <div>When the link state advertisement is describing a router, the link state ID is always the described router's OSPF router ID.</div> <div>When an autonomous system external advertisement (LS Type = 5) is describing a default route, its link state ID is set to Default Destination (0.0.0.0).</div>		

Copyright Registration Information	Cisco	Arista															
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<p>show ip ospf interface</p> <p>To display interface information related to Open Shortest Path First (OSPF), use the show ip ospf interface command in user EXEC or privileged EXEC mode.</p> <p>show ip [ospf] [process-id] interface [type number] [brief] [multicast] [topology {topology-name} base]</p> <table border="1"> <thead> <tr> <th data-bbox="302 427 422 443">Syntax Description</th><th></th><th></th></tr> </thead> <tbody> <tr> <td><i>process-id</i></td><td></td><td>(Optional) Process ID number. If this argument is included, only information for the specified routing process is included. The range is 1 to 65535.</td></tr> <tr> <td><i>type</i></td><td></td><td>(Optional) Interface type. If the <i>type</i> argument is included, only information for the specified interface type is included.</td></tr> <tr> <td><i>number</i></td><td></td><td>(Optional) Interface number. If the <i>number</i> argument is included, only information for the specified interface number is included.</td></tr> <tr> <td>brief</td><td></td><td>(Optional) Displays brief overview information for OSPF interfaces, states, addresses and masks, and areas on the device.</td></tr> </tbody> </table> <p>Cisco IOS IP Routing:OSPF Command Reference (2013), at 202.</p>	Syntax Description			<i>process-id</i>		(Optional) Process ID number. If this argument is included, only information for the specified routing process is included. The range is 1 to 65535.	<i>type</i>		(Optional) Interface type. If the <i>type</i> argument is included, only information for the specified interface type is included.	<i>number</i>		(Optional) Interface number. If the <i>number</i> argument is included, only information for the specified interface number is included.	brief		(Optional) Displays brief overview information for OSPF interfaces, states, addresses and masks, and areas on the device.	<p>show ip ospf interface brief</p> <p>The show ip ospf interface brief command displays a summary of OSPFv2 interfaces, states, addresses and masks, and areas on the router.</p> <p>Platform all Command Mode EXEC</p> <p>Command Syntax</p> <p>show ip ospf [PROCESS ID] interface brief [VRF_INSTANCE]</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1458.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1244; Arista User Manual, v. 4.11.1 (1/11/13), at 1000; Arista User Manual v. 4.10.3 (10/22/12), at 829; Arista User Manual v. 4.9.3.2 (5/3/12), at 653; Arista User Manual v. 4.8.2 (11/18/11), at 488; Arista User Manual v. 4.7.3 (7/18/11), at 360.</p>
Syntax Description																	
<i>process-id</i>		(Optional) Process ID number. If this argument is included, only information for the specified routing process is included. The range is 1 to 65535.															
<i>type</i>		(Optional) Interface type. If the <i>type</i> argument is included, only information for the specified interface type is included.															
<i>number</i>		(Optional) Interface number. If the <i>number</i> argument is included, only information for the specified interface number is included.															
brief		(Optional) Displays brief overview information for OSPF interfaces, states, addresses and masks, and areas on the device.															

Copyright Registration Information	Cisco	Arista						
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<div>shutdown (router OSPF)</div> <p>To initiate a graceful shutdown of the Open Shortest Path First (OSPF) protocol under the current instance, use the shutdown command in router configuration mode. To restart the OSPF protocol, use the noform of this command</p> <div>shutdown no shutdown</div> <div>Syntax Description</div> <p>This command has no arguments or keywords.</p> <div>Command Default</div> <p>OSPF stays active under the current instance.</p> <div>Command Modes</div> <p>Router configuration (config-router)</p> <div>Command History</div> <table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>12.2(33)SRC</td><td>This command was introduced.</td></tr><tr><td>15.0(1)M</td><td>This command was integrated into Cisco IOS Release 15.0(1)M.</td></tr></tbody></table> <div>Usage Guidelines</div> <p>Use the shutdown command in router configuration mode to temporarily shut down a protocol in the least disruptive manner and to notify its neighbors that it is going away. All traffic that has another path through the network will be directed to that alternate path.</p> <p>Cisco IOS IP Routing:OSPF Command Reference (2013), at 252</p>	Release	Modification	12.2(33)SRC	This command was introduced.	15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.	<div>shutdown (OSPFv2)</div> <p>The shutdown command disables OSPFv2 on the switch. Neighbor routers are notified of the shutdown and all traffic that has another path through the network will be directed to an alternate path.</p> <p>OSPFv2 is disabled on individual interfaces with the shutdown (OSPFv2) command.</p> <p>The no shutdown and default shutdown commands enable the OSPFv2 instance by removing the shutdown statement from the OSPF block in <i>running-config</i>.</p> <div>Platform</div> <p>all</p> <div>Command Mode</div> <p>Router-OSPF Configuration</p> <div>Command Syntax</div> <div>shutdown no shutdown default shutdown</div> <p>Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1468</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1253; Arista User Manual, v. 4.11.1 (1/11/13), at 1005; Arista User Manual v. 4.10.3 (10/22/12), at 834; Arista User Manual v. 4.9.3.2 (5/3/12), at 658; Arista User Manual v. 4.8.2 (11/18/11), at 493; Arista User Manual v. 4.7.3 (7/18/11), at 365; Arista User Manual v. 4.6.0 (12/22/2010), at 224</p>
	Release	Modification						
12.2(33)SRC	This command was introduced.							
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.							

Copyright Registration Information	Cisco	Arista			
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<p>timers lsa arrival</p> <p>To set the minimum interval at which the software accepts the same link-state advertisement (LSA) from Open Shortest Path First (OSPF) neighbors, use the <code>timers lsa arrival</code> command in router configuration mode. To restore the default value, use the <code>no</code> form of this command.</p> <p><code>timers lsa arrival milliseconds</code> <code>no timers lsa arrival</code></p> <table border="1"> <tr> <td data-bbox="310 480 428 496">Syntax Description</td><td data-bbox="449 487 533 503"><i>milliseconds</i></td><td data-bbox="772 487 1087 558">Minimum delay in milliseconds that must pass between acceptance of the same LSA arriving from neighbors. The range is from 0 to 600,000 milliseconds. The default is 1000 milliseconds.</td></tr> </table> <p>Cisco IOS IP Routing:OSPF Command Reference (2013), at 286.</p>	Syntax Description	<i>milliseconds</i>	Minimum delay in milliseconds that must pass between acceptance of the same LSA arriving from neighbors. The range is from 0 to 600,000 milliseconds. The default is 1000 milliseconds.	<p>timers lsa arrival (OSPFv2)</p> <p>The <code>timers lsa arrival</code> command sets the minimum interval in which the switch accepts the same link-state advertisement (LSA) from OSPF neighbors.</p> <p>The <code>no timers lsa arrival</code> and default <code>timers lsa arrival</code> commands restore the default maximum OSPFv2 path calculation interval to five seconds by removing the <code>timers lsa arrival</code> command from <i>running-config</i>.</p> <p>Platform all Command Mode Router-OSPF Configuration</p> <p>Command Syntax</p> <p><code>timers lsa arrival lsa_time</code> <code>no timers lsa arrival</code> <code>default timers lsa arrival</code></p> <p>Parameters</p> <ul style="list-style-type: none"> <i>lsa_time</i> OSPFv2 minimum interval (seconds). Values range from 1 to 600000 milliseconds. Default is 1000 milliseconds. <p>Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1469.</p>
Syntax Description	<i>milliseconds</i>	Minimum delay in milliseconds that must pass between acceptance of the same LSA arriving from neighbors. The range is from 0 to 600,000 milliseconds. The default is 1000 milliseconds.			

Copyright Registration Information	Cisco	Arista						
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<p>timers basic (RIP)</p> <p>To adjust Routing Information Protocol (RIP) network timers, use the <code>timers basic</code> command in router configuration mode. To restore the default timers, use the <code>no</code> form of this command.</p> <p><code>timers basic</code> <i>update invalid holddown flush</i> <code>no timers basic</code></p> <table border="1"> <tr> <td data-bbox="296 456 420 475">Syntax Description</td><td data-bbox="443 456 491 475"><i>update</i></td><td data-bbox="768 456 1087 516">Rate (in seconds) at which updates are sent. This is the fundamental timing parameter of the routing protocol. The default is 30 seconds.</td></tr> <tr> <td></td><td data-bbox="443 529 491 548"><i>invalid</i></td><td data-bbox="768 529 1087 691">Interval of time (in seconds) after which a route is declared invalid; it should be at least three times the value of the <i>update</i> argument. A route becomes invalid when there is an absence of updates that refresh the route. The route then enters into a <i>holddown</i> state. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets. The default is 180 seconds.</td></tr> </table> <p>Cisco IOS IP Routing:RIP Command Reference (2013), at 56.</p>	Syntax Description	<i>update</i>	Rate (in seconds) at which updates are sent. This is the fundamental timing parameter of the routing protocol. The default is 30 seconds.		<i>invalid</i>	Interval of time (in seconds) after which a route is declared invalid; it should be at least three times the value of the <i>update</i> argument. A route becomes invalid when there is an absence of updates that refresh the route. The route then enters into a <i>holddown</i> state. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets. The default is 180 seconds.	<p>timers basic (RIP)</p> <p>The <code>timers basic</code> command configures the update interval, the expiration time, and the deletion time for routes received and sent through RIP. The command requires value declaration of all values.</p> <ul style="list-style-type: none"> The update time is the interval between unsolicited route responses. The default is 30 seconds. The expiration time is initialized when a route is established and any time an update is received for the route. If the specified period elapses from the last time the route update was received, then the route is marked as inaccessible and advertised as unreachable. However, the route forwards packets until the deletion time expires. The default value is 180 seconds. The deletion time is initialized when the expiration time has elapsed. On initialization of the deletion time, the route is no longer valid; however, it is retained in the routing table for a short time so that neighbors can be notified that the route has been dropped. Upon expiration of the deletion time, the route is removed from the routing table. The default is 120 seconds. <p>The <code>no timers basic</code> and default <code>timers basic</code> commands return the timer values to their default values by removing the <code>timers-basic</code> command from <i>running-config</i>.</p> <p>Platform all Command Mode Router-RIP Configuration</p> <p>Command Syntax</p> <p><code>timers basic</code> <i>update_time expire_time deletion_time</i> <code>no timers basic</code> <code>default timers basic</code></p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1671.</p> <p><i>See also</i> Arista User Manual v. 4.13.6F (4/14/2014), at 1621; Arista User Manual v. 4.12.3 (7/17/13), at 1433; Arista User Manual, v. 4.11.1 (1/11/13), at 1179; Arista User Manual v. 4.10.3 (10/22/12), at 989; Arista User Manual v. 4.9.3.2 (5/3/12), at 748; Arista User Manual v. 4.8.2 (11/18/11), at 570.</p>
Syntax Description	<i>update</i>	Rate (in seconds) at which updates are sent. This is the fundamental timing parameter of the routing protocol. The default is 30 seconds.						
	<i>invalid</i>	Interval of time (in seconds) after which a route is declared invalid; it should be at least three times the value of the <i>update</i> argument. A route becomes invalid when there is an absence of updates that refresh the route. The route then enters into a <i>holddown</i> state. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets. The default is 180 seconds.						

Copyright Registration Information	Cisco	Arista						
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<p>distance (IPv6 EIGRP)</p> <p>To allow the use of two administrative distances—internal and external—that could be a better route to a node, use the <code>distance</code> command in router configuration mode. To reset these values to their defaults, use the <code>no distance</code> form of this command.</p> <p><code>distance</code> <i>internal-distance external-distance</i> <code>no distance</code></p> <table border="1"> <tr> <td data-bbox="306 483 428 500">Syntax Description</td><td data-bbox="449 488 562 505"><i>internal-distance</i></td><td data-bbox="785 488 1108 581">Administrative distance for Enhanced Internal Gateway Routing Protocol (EIGRP) for IPv6 internal routes. Internal routes are those that are learned from another entity within the same autonomous system. The distance can be a value from 1 to 255.</td></tr> <tr> <td></td><td data-bbox="449 597 562 613"><i>external-distance</i></td><td data-bbox="785 597 1108 690">Administrative distance for EIGRP for IPv6 external routes. External routes are those for which the best path is learned from a neighbor external to the autonomous system. The distance can be a value from 1 to 255.</td></tr> </table> <p>Cisco IOS IP Routing: EIGRP Command Reference (2013), at 42.</p>	Syntax Description	<i>internal-distance</i>	Administrative distance for Enhanced Internal Gateway Routing Protocol (EIGRP) for IPv6 internal routes. Internal routes are those that are learned from another entity within the same autonomous system. The distance can be a value from 1 to 255.		<i>external-distance</i>	Administrative distance for EIGRP for IPv6 external routes. External routes are those for which the best path is learned from a neighbor external to the autonomous system. The distance can be a value from 1 to 255.	<p>distance <code>bgp</code></p> <p>The <code>distance bgp</code> command assigns an administrative distance to routes that the switch learns through BGP. Routers use administrative distances to select a route when two protocols provide routing information to the same destination. Distance values range from 1 to 255; lower distance values correspond to higher reliability. BGP routing tables do not include routes with a distance of 255.</p> <p>The <code>distance</code> command assigns distance values to external, internal, and local BGP routes:</p> <ul style="list-style-type: none"> external: External routes are routes for which the best path is learned from a neighbor external to the autonomous system. Default distance is 200. internal: Internal routes are routes learned from a BGP entity within the same autonomous system. Default distance is 200. local: Local routes are networks listed with a network router configuration command for that router or for networks that are redistributed from another process. Default distance is 200. <p>The <code>no distance bgp</code> and <code>default distance bgp</code> commands restore the default administrative distances by removing the <code>distance bgp</code> command from <i>running-config</i>.</p> <p>Platform all Command Mode Router-BGP Configuration</p> <p>Command Syntax</p> <p><code>distance</code> <code>bgp</code> <i>external_dist</i> [<i>INTERNAL_LOCAL</i>] <code>no distance</code> <code>bgp</code> <code>default distance</code> <code>bgp</code></p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1583.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1360; Arista User Manual, v. 4.11.1 (1/11/13), at 1106; Arista User Manual v. 4.10.3 (10/22/12), at 918; Arista User Manual v. 4.9.3.2 (5/3/12), at 684; Arista User Manual v. 4.8.2 (11/18/11), at 514; Arista User Manual v. 4.7.3 (7/18/11), at 379.</p>
Syntax Description	<i>internal-distance</i>	Administrative distance for Enhanced Internal Gateway Routing Protocol (EIGRP) for IPv6 internal routes. Internal routes are those that are learned from another entity within the same autonomous system. The distance can be a value from 1 to 255.						
	<i>external-distance</i>	Administrative distance for EIGRP for IPv6 external routes. External routes are those for which the best path is learned from a neighbor external to the autonomous system. The distance can be a value from 1 to 255.						

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<p>Extended community attributes are used to configure, filter, and identify routes for virtual routing and forwarding instances (VRFs) and Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs). The match extcommunity command is used to configure match clauses that use extended community attributes in route maps. All of the standard rules of match and set clauses apply to the configuration of extended community attributes.</p> <p>Cisco IOS IP Routing: EIGRP Command Reference (2013), at 130.</p>	<p>BGP extended communities configure, filter, and identify routes for virtual routing, forwarding instances (VRFs), and Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs).</p> <p>Extended community clauses provide route target and site of origin parameter options:</p> <ul style="list-style-type: none"> • route targets (rt): This attribute identifies a set of sites and VRFs that may receive routes tagged with the configured route target. Configuring this attribute with a route allows that route to be placed in per-site forwarding tables that route traffic received from corresponding sites. • site of origin (soo): This attribute identifies the site from where the Provider Edge (PE) router learns the route. All routes learned from a specific site have the same SOO extended community attribute, whether a site is connected to a single or multiple PE routers. This attribute prevents routing loops resulting from multihomed sites. The SOO attribute is configured on the interface and propagated into a BGP domain by redistribution. The SOO is applied to routes learned from VRFs. <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1552.</p> <p><i>See also</i> Arista User Manual v. 4.13.6F (4/14/2014), at 1502; Arista User Manual v. 4.12.3 (7/17/13), at 1334; Arista User Manual, v. 4.11.1 (1/11/13), at 1083-84; Arista User Manual v. 4.10.3 (10/22/12), at 896; Arista User Manual v. 4.9.3.2 (5/3/12), at 668; Arista User Manual v. 4.8.2 at 500.</p>
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<p>shutdown (address-family)</p> <p>To disable the Enhanced Interior Gateway Routing Protocol (EIGRP) address-family protocol for a specific routing instance without removing any existing address-family configuration parameters, use the shutdown command in the appropriate configuration mode. To reenable the EIGRP address-family protocol, use the no form of this command.</p> <p>Cisco IOS IP Routing: EIGRP Command Reference (2013), at 276.</p>	<p>29.3.4 Disabling IS-IS</p> <p>The IS-IS protocol can be disabled globally on on individual interfaces.</p> <p>The shutdown (IS-IS) command disables the IS-IS protocol for a specific routing instance without removing any existing IS-IS configuration parameters.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1679.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1440.</p>

Copyright Registration Information	Cisco		Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<div>maximum-paths</div>	Controls the maximum number of parallel routes an IP routing protocol can support.	<div>maximum-paths (OSPFv2)</div> <div>The maximum-paths command controls the maximum number of parallel routes that OSPFv2 supports on the switch. The default maximum is 16 paths.</div> <div>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1440.</div> <div>See also Arista User Manual v. 4.12.3 (7/17/13), at 1226; Arista User Manual, v. 4.11.1 (1/11/13), at 983; Arista User Manual v. 4.10.3 (10/22/12), at 813; Arista User Manual v. 4.9.3.2 (5/3/12), at 637; Arista User Manual v. 4.8.2 (11/18/11), at 472.</div>
	Cisco IOS IP Routing: BGP Command Reference (2013), at 375.		
Cisco IOS 12.4 Effective date of registration: 8/12/2005	<div>maximum-paths</div>	Controls the maximum number of parallel routes an IP routing protocol can support.	<div>maximum-paths (OSPFv2)</div> <div>The maximum-paths command controls the maximum number of parallel routes that OSPFv2 supports on the switch. The default maximum is 16 paths.</div> <div>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1440.</div> <div>See also Arista User Manual v. 4.12.3 (7/17/13), at 1226; Arista User Manual, v. 4.11.1 (1/11/13), at 983; Arista User Manual v. 4.10.3 (10/22/12), at 813; Arista User Manual v. 4.9.3.2 (5/3/12), at 637; Arista User Manual v. 4.8.2 (11/18/11), at 472.</div>
	Cisco IOS IP Routing Protocols Command Reference (June 10, 2005), at 146.		

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<p>Together, a route reflector and its clients form a <i>cluster</i>. When a single route reflector is deployed in a cluster, the cluster is identified by the router ID of the route reflector.</p> <p>The <code>bgp cluster-id</code> command is used to assign a cluster ID to a route reflector when the cluster has one or more route reflectors. Multiple route reflectors are deployed in a cluster to increase redundancy and avoid a single point of failure. When multiple route reflectors are configured in a cluster, the same cluster ID is assigned to all route reflectors. This allows all route reflectors in the cluster to recognize updates from peers in the same cluster and reduces the number of updates that need to be stored in BGP routing tables.</p> <p>Cisco IOS IP Routing: BGP Command Reference (2013), at 74.</p>	<p>When using route reflectors, an AS is divided into clusters. A cluster consists of one or more route reflectors and a group of clients to which they re-advertise route information. Multiple route reflectors can be configured in the same cluster to increase redundancy and avoid a single point of failure. Each route reflector has a cluster ID. If the cluster has a single route reflector, the cluster ID is its router ID. If a cluster has multiple route reflectors, a 4-byte cluster ID is assigned to all route reflectors in the cluster. All of them must be configured with the same cluster ID so that they can recognize updates from other route reflectors in the same cluster. The <code>bgp cluster-id</code> command configures the cluster ID in a cluster with multiple route reflectors.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1549.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1331; Arista User Manual, v. 4.11.1 (1/11/13), at 1081; Arista User Manual v. 4.10.3 (10/22/12), at 893; Arista User Manual v. 4.9.3.2 (5/3/12), at 665.</p>
<p>Cisco IOS 12.4</p> <p>Effective date of registration: 8/12/2005</p>	<p>Together, a route reflector and its clients form a <i>cluster</i>. When a single route reflector is deployed in a cluster, the cluster is identified by the router ID of the route reflector.</p> <p>The <code>bgp cluster-id</code> command is used to assign a cluster ID to a route reflector when the cluster has one or more route reflectors. Multiple route reflectors are deployed in a cluster to increase redundancy and avoid a single point of failure. When multiple route reflectors are configured in a cluster, the same cluster ID is assigned to all route reflectors. This allows all route reflectors in the cluster to recognize updates from peers in the same cluster and reduces the number of updates that need to be stored in BGP routing tables.</p> <p>Cisco IOS IP Routing Protocols Command Reference (July 16, 2005), at 25.</p>	<p>When using route reflectors, an AS is divided into clusters. A cluster consists of one or more route reflectors and a group of clients to which they re-advertise route information. Multiple route reflectors can be configured in the same cluster to increase redundancy and avoid a single point of failure. Each route reflector has a cluster ID. If the cluster has a single route reflector, the cluster ID is its router ID. If a cluster has multiple route reflectors, a 4-byte cluster ID is assigned to all route reflectors in the cluster. All of them must be configured with the same cluster ID so that they can recognize updates from other route reflectors in the same cluster. The <code>bgp cluster-id</code> command configures the cluster ID in a cluster with multiple route reflectors.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1549.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1331; Arista User Manual, v. 4.11.1 (1/11/13), at 1081; Arista User Manual v. 4.10.3 (10/22/12), at 893; Arista User Manual v. 4.9.3.2 (5/3/12), at 665.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<p>The bgp confederation identifier command is used to configure a single autonomous system number to identify a group of smaller autonomous systems as a single confederation.</p> <p>A confederation can be used to reduce the internal BGP (iBGP) mesh by dividing a large single autonomous system into multiple subautonomous systems and then grouping them into a single confederation. The subautonomous systems within the confederation exchange routing information like iBGP peers. External peers interact with the confederation as if it were a single autonomous system.</p> <p>Each subautonomous system is fully meshed within itself and has a few connections to other autonomous systems within the confederation. Next hop, Multi Exit Discriminator (MED), and local preference information is preserved throughout the confederation, allowing you to retain a single Interior Gateway Protocol (IGP) for all the autonomous systems</p> <p>Cisco IOS IP Routing: BGP Command Reference (2013), at 77</p>	<p>BGP Confederations</p> <p>BGP confederations allow you to break an autonomous system into multiple sub-autonomous systems, and then to group the sub-autonomous systems as a confederation.</p> <p>The sub-autonomous systems exchange routing information as if they are iBGP peers. Specifically, routing updates between sub-autonomous systems include the next-hop, local-preference and MED attributes.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1556.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1326.</p>
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<p>bgp redistribute-internal</p> <p>To configure iBGP redistribution into an interior gateway protocol (IGP), such as IS-IS or OSPF, use the bgp redistribute-internal command in address family or router configuration mode. To stop iBGP redistribution into IGPs, use the no form of this command.</p> <p>bgp redistribute-internal no bgp redistribute-internal</p> <p>Cisco IOS IP Routing: BGP Command Reference (2013), at 133</p>	<p>bgp redistribute-internal (BGP)</p> <p>The bgp redistribute-internal command enables iBGP redistribution into an interior gateway protocol (IGP), such as IS-IS or OSPF in address family or router BGP configuration mode.</p> <p>The no bgp redistribute-internal and default bgp redistribute-internal commands disable route redistribution from the specified domain by removing the corresponding bgp redistribute-internal command from <i>running-config</i>.</p> <p>Platform all Command Mode Router-BGP Configuration Router-BGP Configuration-Address-Family</p> <p>Command Syntax</p> <p>bgp redistribute internal no bgp redistribute internal default bgp redistribute internal</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1576.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1357.</p>

Copyright Registration Information	Cisco	Arista						
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<div>bgp router-id</div> <div>To configure a fixed router ID for the local Border Gateway Protocol (BGP) routing process, use the bgp router-id command in router or address family configuration mode. To remove the fixed router ID from the running configuration file and restore the default router ID selection, use the no form of this command.</div> <div>Router Configuration bgp router-id {ip-address} vrf auto-assign} no bgp router-id [vrf auto-assign]</div> <div>Address Family Configuration bgp router-id {ip-address} auto-assign} no bgp router-id</div> <div>Syntax Description<table><tr><td>ip-address</td><td>Router identifier in the form of an IP address.</td></tr><tr><td>vrf</td><td>Configures a router identifier for a Virtual Routing and Forwarding (VRF) instance.</td></tr><tr><td>auto-assign</td><td>Automatically assigns a router identifier for each VRF.</td></tr></table></div> <div>Command Default<div>The following behavior determines local router ID selection when this command is not enabled:<ul style="list-style-type: none">If a loopback interface is configured, the router ID is set to the IP address of the loopback interface. If multiple loopback interfaces are configured, the router ID is set to the IP address of the loopback interface with the highest IP address.If no loopback interface is configured, the router ID is set to the highest IP address on a physical interface.</div></div> <div>Cisco IOS IP Routing: BGP Command Reference (2013), at 142.</div>	ip-address	Router identifier in the form of an IP address.	vrf	Configures a router identifier for a Virtual Routing and Forwarding (VRF) instance.	auto-assign	Automatically assigns a router identifier for each VRF.	<div>router-id (BGP)</div> <div>The router-id command configures a fixed router ID for the local Border Gateway Protocol (BGP) routing process.</div> <div>When the router-id command is not configured, the local router ID is set to the following:<ul style="list-style-type: none">The loopback IP address when a loopback interface is configured. The loopback with the highest IP address is selected when multiple loopback interfaces are configured.The highest IP address on a physical interface when no loopback interfaces are configured.</div> <div>Important The router-id must be specified if the switch has no IPv4 addresses configured.</div> <div>The no router-id and default router-id commands remove the router-id command from running-config.</div> <div>Platform all Command Mode Router-BGP Configuration</div> <div>Command Syntax router-id id_num no router-id [id_num] default router-id [id_num]</div> <div>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1625.</div> <div>See also Arista User Manual v. 4.12.3 (7/17/13), at 1397; Arista User Manual, v. 4.11.1 (1/11/13), at 1143; Arista User Manual v. 4.10.3 (10/22/12), at 954; Arista User Manual v. 4.9.3.2 (5/3/12), at 716.</div>
	ip-address	Router identifier in the form of an IP address.						
	vrf	Configures a router identifier for a Virtual Routing and Forwarding (VRF) instance.						
auto-assign	Automatically assigns a router identifier for each VRF.							

Copyright Registration Information	Cisco	Arista		
Cisco IOS 12.4 Effective date of registration: 8/12/2005	bgp router-id <div>To configure a fixed router ID for the local Border Gateway Protocol (BGP) routing process, use the bgp router-id command in router configuration mode. To remove the fixed router ID from the running configuration file and restore the default router ID selection, use the no form of this command.</div> <div>bgp router-id <i>ip-address</i> no bgp router-id <i>ip-address</i></div> <table><tr><td>Syntax Description</td><td><i>ip-address</i> IP address of the router.</td></tr></table> <div>Defaults<div>The following behavior determines local router ID selection when this command is not enabled:<ul style="list-style-type: none">If a loopback interface is configured, the router ID is set to the IP address of the loopback. If multiple loopback interfaces are configured, the loopback with the highest IP address is used.If no loopback interface is configured, the router ID is set to the highest IP address on a physical interface.</div></div>	Syntax Description	<i>ip-address</i> IP address of the router.	<div>router-id (BGP) The router-id command configures a fixed router ID for the local Border Gateway Protocol (BGP) routing process. When the router-id command is not configured, the local router ID is set to the following:<ul style="list-style-type: none">The loopback IP address when a loopback interface is configured. The loopback with the highest IP address is selected when multiple loopback interfaces are configured.The highest IP address on a physical interface when no loopback interfaces are configured.</div> <div>Important The router-id must be specified if the switch has no IPv4 addresses configured.</div> <div>The no router-id and default router-id commands remove the router-id command from <i>running-config</i>. Platform all Command Mode Router-BGP Configuration Command Syntax<div>router-id <i>id_num</i> no router-id [<i>id_num</i>] default router-id [<i>id_num</i>]</div></div>
	Syntax Description	<i>ip-address</i> IP address of the router.		
		Cisco IOS IP Routing Protocols Command Reference (July 16, 2005), at 55.	Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1625.	
		See also Arista User Manual v. 4.12.3 (7/17/13), at 1397; Arista User Manual, v. 4.11.1 (1/11/13), at 1143; Arista User Manual v. 4.10.3 (10/22/12), at 954; Arista User Manual v. 4.9.3.2 (5/3/12), at 716.		

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<p>The clear ip bgp command can be used to initiate a hard reset or soft reconfiguration. A hard reset tears down and rebuilds the specified peering sessions and rebuilds the BGP routing tables. A soft reconfiguration uses stored prefix information to reconfigure and activate BGP routing tables without tearing down existing peering sessions. Soft reconfiguration uses stored update information at the cost of additional memory for storing the updates, to allow you to apply new BGP policy without disrupting the network. Soft reconfiguration can be configured for inbound or outbound sessions.</p> <p>Cisco IOS IP Routing: BGP Command Reference (2013), at 193</p>	<p>clear ip bgp</p> <p>The clear ip bgp command removes BGP IPv4 learned routes from the routing table, reads all routes from designated peers, and sends routes to those peers as required.</p> <ul style="list-style-type: none"> • a hard reset tears down and rebuilds the peering sessions and rebuilds BGP routing tables. • a soft reset uses stored prefix information to reconfigure and activate BGP routing tables without tearing down existing peering sessions. <p>Soft resets use stored update information to apply new BGP policy without disrupting the network.</p> <p>Routes that are read or sent are processed through modified route maps or AS-path access lists. The command can also clear the switch's BGP sessions with its peers.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) 10/2/2014), at 1577.</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 1527; Arista User Manual v. 4.12.3 (7/17/13), at 1358; Arista User Manual, v. 4.11.1 (1/11/13), at 1104; Arista User Manual v. 4.10.3 (10/22/12), at 916; Arista User Manual v. 4.9.3.2 (5/3/12), at 683; Arista User Manual v. 4.8.2 (11/18/11), at 513; Arista User Manual v. 4.7.3 (7/18/11), at 378.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 12.4</p> <p>Effective date of registration: 8/12/2005</p>	<p>The clear ip bgp command can be used to initiate a hard reset or soft reconfiguration. A hard reset tears down and rebuilds the specified peering sessions and rebuilds the BGP routing tables. A soft reconfiguration uses stored prefix information to reconfigure and activate BGP routing tables without tearing down existing peering sessions. Soft reconfiguration uses stored update information, at the cost of additional memory for storing the updates, to allow you to apply new BGP policy without disrupting the network. Soft reconfiguration can be configured for inbound or outbound sessions.</p> <p>Cisco IOS IP Routing Protocols Command Reference (July 16, 2005), at 72-73.</p>	<p>clear ip bgp</p> <p>The clear ip bgp command removes BGP IPv4 learned routes from the routing table, reads all routes from designated peers, and sends routes to those peers as required.</p> <ul style="list-style-type: none"> • a hard reset tears down and rebuilds the peering sessions and rebuilds BGP routing tables. • a soft reset uses stored prefix information to reconfigure and activate BGP routing tables without tearing down existing peering sessions. <p>Soft resets use stored update information to apply new BGP policy without disrupting the network.</p> <p>Routes that are read or sent are processed through modified route maps or AS-path access lists. The command can also clear the switch's BGP sessions with its peers.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) 10/2/2014), at 1577.</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 1527; Arista User Manual v. 4.12.3 (7/17/13), at 1358; Arista User Manual, v. 4.11.1 (1/11/13), at 1104; Arista User Manual v. 4.10.3 (10/22/12), at 916; Arista User Manual v. 4.9.3.2 (5/3/12), at 683; Arista User Manual v. 4.8.2 (11/18/11), at 513; Arista User Manual v. 4.7.3 (7/18/11), at 378.</p>

Copyright Registration Information	Cisco	Arista						
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<div>distance bgp</div> <p>To configure the administrative distance for BGP routes, use the distance bgp command in address family or router configuration mode. To return to the administrative distance to the default value, use the no form of this command.</p> <div>distance bgp external-distance internal-distance local-distance no distance bgp</div> <div>Syntax Description</div> <table><tr><td>external-distance</td><td>Administrative distance for external BGP routes. Routes are external when learned from an external autonomous system. The range of values for this argument are from 1 to 255.</td></tr><tr><td>internal-distance</td><td>Administrative distance for internal BGP routes. Routes are internal when learned from peer in the local autonomous system. The range of values for this argument are from 1 to 255.</td></tr><tr><td>local-distance</td><td>Administrative distance for local BGP routes. Local routes are those networks listed with a network router configuration command, often as back doors, for the router or for the networks that is being redistributed from another process. The range of values for this argument are from 1 to 255.</td></tr></table> <p>Cisco IOS IP Routing: BGP Command Reference (2013), at 271.</p>	external-distance	Administrative distance for external BGP routes. Routes are external when learned from an external autonomous system. The range of values for this argument are from 1 to 255.	internal-distance	Administrative distance for internal BGP routes. Routes are internal when learned from peer in the local autonomous system. The range of values for this argument are from 1 to 255.	local-distance	Administrative distance for local BGP routes. Local routes are those networks listed with a network router configuration command, often as back doors, for the router or for the networks that is being redistributed from another process. The range of values for this argument are from 1 to 255.	<div>distance bgp</div> <p>The distance bgp command assigns an administrative distance to routes that the switch learns through BGP. Routers use administrative distances to select a route when two protocols provide routing information to the same destination. Distance values range from 1 to 255; lower distance values correspond to higher reliability. BGP routing tables do not include routes with a distance of 255.</p> <p>The distance command assigns distance values to external, internal, and local BGP routes:</p> <ul style="list-style-type: none">external: External routes are routes for which the best path is learned from a neighbor external to the autonomous system. Default distance is 200.internal: Internal routes are routes learned from a BGP entity within the same autonomous system. Default distance is 200.local: Local routes are networks listed with a network router configuration command for that router or for networks that are redistributed from another process. Default distance is 200. <p>The no distance bgp and default distance bgp commands restore the default administrative distances by removing the distance bgp command from running-config.</p> <p>Platform all Command Mode Router-BGP Configuration</p> <p>Command Syntax</p> <div>distance bgp external_dist [INTERNAL_LOCAL] no distance bgp default distance bgp</div> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1583.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1360; Arista User Manual, v. 4.11.1 (1/11/13), at 1106; Arista User Manual v. 4.10.3 (10/22/12), at 918; Arista User Manual v. 4.9.3.2 (5/3/12), at 684; Arista User Manual v. 4.8.2 (11/18/11), at 514; Arista User Manual v. 4.7.3 (7/18/11), at 379.</p>
	external-distance	Administrative distance for external BGP routes. Routes are external when learned from an external autonomous system. The range of values for this argument are from 1 to 255.						
internal-distance	Administrative distance for internal BGP routes. Routes are internal when learned from peer in the local autonomous system. The range of values for this argument are from 1 to 255.							
local-distance	Administrative distance for local BGP routes. Local routes are those networks listed with a network router configuration command, often as back doors, for the router or for the networks that is being redistributed from another process. The range of values for this argument are from 1 to 255.							

Copyright Registration Information	Cisco	Arista									
<p>Cisco IOS 12.4</p> <p>Effective date of registration: 8/12/2005</p>	<p>distance bgp</p> <p>To configure the administrative distance for BGP routes, use the distance bgp command in address family or router configuration mode. To return to the administrative distance to the default value, use the no form of this command.</p> <pre>distance bgp external-distance internal-distance local-distance no distance bgp</pre> <table border="1"> <tr> <td>Syntax Description</td><td><i>external-distance</i></td><td>Administrative distance for external BGP routes. Routes are external when learned from an external autonomous system. The range of values for this argument are from 1 to 255.</td></tr> <tr> <td></td><td><i>internal-distance</i></td><td>Administrative distance for internal BGP routes. Routes are internal when learned from peer in the local autonomous system. The range of values for this argument are from 1 to 255.</td></tr> <tr> <td></td><td><i>local-distance</i></td><td>Administrative distance for local BGP routes. Local routes are those networks listed with a network router configuration command, often as back doors, for the router or for the networks that is being redistributed from another process. The range of values for this argument are from 1 to 255.</td></tr> </table> <p>Cisco IOS IP Routing Protocols Command Reference (July 16, 2005), at 95.</p>	Syntax Description	<i>external-distance</i>	Administrative distance for external BGP routes. Routes are external when learned from an external autonomous system. The range of values for this argument are from 1 to 255.		<i>internal-distance</i>	Administrative distance for internal BGP routes. Routes are internal when learned from peer in the local autonomous system. The range of values for this argument are from 1 to 255.		<i>local-distance</i>	Administrative distance for local BGP routes. Local routes are those networks listed with a network router configuration command, often as back doors, for the router or for the networks that is being redistributed from another process. The range of values for this argument are from 1 to 255.	<p>distance bgp</p> <p>The distance bgp command assigns an administrative distance to routes that the switch learns through BGP. Routers use administrative distances to select a route when two protocols provide routing information to the same destination. Distance values range from 1 to 255; lower distance values correspond to higher reliability. BGP routing tables do not include routes with a distance of 255.</p> <p>The distance command assigns distance values to external, internal, and local BGP routes:</p> <ul style="list-style-type: none"> external: External routes are routes for which the best path is learned from a neighbor external to the autonomous system. Default distance is 200. internal: Internal routes are routes learned from a BGP entity within the same autonomous system. Default distance is 200. local: Local routes are networks listed with a network router configuration command for that router or for networks that are redistributed from another process. Default distance is 200. <p>The no distance bgp and default distance bgp commands restore the default administrative distances by removing the distance bgp command from <i>running-config</i>.</p> <p>Platform all Command Mode Router-BGP Configuration</p> <p>Command Syntax</p> <pre>distance bgp external_dist [INTERNAL_LOCAL] no distance bgp default distance bgp</pre> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1583.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1360; Arista User Manual, v. 4.11.1 (1/11/13), at 1106; Arista User Manual v. 4.10.3 (10/22/12), at 918; Arista User Manual v. 4.9.3.2 (5/3/12), at 684; Arista User Manual v. 4.8.2 (11/18/11), at 514; Arista User Manual v. 4.7.3 (7/18/11), at 379.</p>
Syntax Description	<i>external-distance</i>	Administrative distance for external BGP routes. Routes are external when learned from an external autonomous system. The range of values for this argument are from 1 to 255.									
	<i>internal-distance</i>	Administrative distance for internal BGP routes. Routes are internal when learned from peer in the local autonomous system. The range of values for this argument are from 1 to 255.									
	<i>local-distance</i>	Administrative distance for local BGP routes. Local routes are those networks listed with a network router configuration command, often as back doors, for the router or for the networks that is being redistributed from another process. The range of values for this argument are from 1 to 255.									

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<p>Expanded Community Lists</p> <p>Expanded community lists are used to filter communities using a regular expression. Regular expressions are used to configure patterns to match community attributes. <u>The order for matching using the * or + character is longest construct first. Nested constructs are matched from the outside in. Concatenated constructs are matched beginning at the left side. If a regular expression can match two different parts of an input string, it will match the earliest part first.</u> For more information about configuring regular expressions, see the "Regular Expressions" appendix of the <i>Terminal Services Configuration Guide</i>.</p> <p>Cisco IOS IP Routing: BGP Command Reference (2013), at 324.</p>	<p><u>The order for matching using the * or + character is longest construct first. Nested constructs are matched from the outside in. Concatenated constructs are matched beginning at the left side. If a regular expression can match two different parts of an input string, it matches the earliest part first.</u></p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 107.</p> <p><i>See also</i> Arista User Manual v. 4.13.6F (4/14/2014), at 105; Arista User Manual v. 4.12.3 (7/17/13), at 95; Arista User Manual, v. 4.11.1 (1/11/13), at 65; Arista User Manual v. 4.10.3 (10/22/12), at 57; Arista User Manual v. 4.9.3.2 (5/3/12), at 53; Arista User Manual v. 4.8.2 (11/18/11), at 49.</p>
<p>Cisco IOS 12.4</p> <p>Effective date of registration: 8/12/2005</p>	<p>Expanded Community Lists</p> <p>Expanded community lists are used to filter communities using a regular expression. Regular expressions are used to configure patterns to match community attributes. <u>The order for matching using the * or + character is longest construct first. Nested constructs are matched from the outside in.</u></p> <p><u>Concatenated constructs are matched beginning at the left side. If a regular expression can match two different parts of an input string, it will match the earliest part first.</u> For more information about configuring regular expressions, see the <i>Regular Expressions</i> appendix of the <i>Cisco IOS Terminal</i></p> <p>Cisco IOS IP Routing Protocols Command Reference (July 16, 2005), at 117-18.</p>	<p><u>The order for matching using the * or + character is longest construct first. Nested constructs are matched from the outside in. Concatenated constructs are matched beginning at the left side. If a regular expression can match two different parts of an input string, it matches the earliest part first.</u></p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 107.</p> <p><i>See also</i> Arista User Manual v. 4.13.6F (4/14/2014), at 105; Arista User Manual v. 4.12.3 (7/17/13), at 95; Arista User Manual, v. 4.11.1 (1/11/13), at 65; Arista User Manual v. 4.10.3 (10/22/12), at 57; Arista User Manual v. 4.9.3.2 (5/3/12), at 53; Arista User Manual v. 4.8.2 (11/18/11), at 49.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<p>ip extcommunity-list</p> <p>To create an extended community list to configure Virtual Private Network (VPN) route filtering, use the ip extcommunity-list command in global configuration mode. To delete the extended community list, use the no form of this command.</p> <p>To enter IP Extended community-list configuration mode to create or configure an extended community-list, use the ip extcommunity-list command in global configuration mode. To delete the entire extended community list, use the no form of this command. To delete a single entry, use the no form in IP Extended community-list configuration mode.</p> <p>Global Configuration Mode CLI</p> <pre>ip extcommunity-list {expanded-list [permit deny] [regular-expression] expanded list-name [permit deny] [regular-expression] standard-list [permit deny] [rt value] [soo value] standard list-name [permit deny] [rt value] [soo value]} no ip extcommunity-list {expanded-list expanded list-name standard-list standard list-name}</pre> <p>ip extcommunity-list {expanded-list expanded list-name standard-list standard list-name} no ip extcommunity-list {expanded-list expanded list-name standard-list standard list-name}</p> <p>Cisco IOS IP Routing: BGP Command Reference (2013), at 326</p>	<p>ip extcommunity-list standard</p> <p>The ip extcommunity-list standard command creates an extended community list to configure Virtual Private Network (VPN) route filtering. Extended community attributes filter routes for virtual routing and forwarding instances (VRFs).</p> <ul style="list-style-type: none"> Route Target (rt) attribute identifies a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that route traffic received from corresponding sites. Site of Origin (soo) attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a specific site must be assigned the same site of origin attribute whether a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents the creation of routing loops when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed. <p>The no ip extcommunity-list standard and default ip extcommunity-list standard commands delete the specified extended community list by removing the corresponding ip extcommunity-list standard statement from <i>running-config</i>.</p> <p>Platform all Command Mode Global Configuration</p> <p>Command Syntax</p> <pre>ip extcommunity-list standard listname FILTER TYPE COMM 1 [COMM 2...COMM n] no ip extcommunity-list standard listname default ip extcommunity-list standard listname</pre> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1591.</p> <p><i>See also</i> Arista User Manual v. 4.13.6F (4/14/2014), at 1541; Arista User Manual v. 4.12.3 (7/17/13), at 1365; Arista User Manual, v. 4.11.1 (1/11/13), at 1111; Arista User Manual v. 4.10.3 (10/22/12), at 923; Arista User Manual v. 4.9.3.2 (5/3/12), at 690; Arista User Manual v. 4.8.2 (11/18/11), at 520.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 12.4</p> <p>Effective date of registration: 8/12/2005</p>	<p>ip extcommunity-list</p> <p>To create an extended community list to configure Virtual Private Network (VPN) route filtering, use the ip extcommunity-list command in global configuration mode. To delete the extended community list, use the no form of this command.</p> <p>Global Configuration Mode CLI</p> <pre>ip extcommunity-list expanded-list / expanded-list-name {permit deny} [regular-expression] / standard-list / standard-list-name {permit deny} [rt value] [soo value]</pre> <pre>no ip extcommunity-list expanded-list / expanded-list-name / standard-list / standard-list-name</pre> <p>To enter IP extended community-list configuration mode to create or configure an extended community-list, use the ip extcommunity-list command in global configuration mode. To delete the entire extended community list, use the no form of this command. To delete a single entry, use the no form in IP Extended community-list configuration mode.</p> <pre>ip extcommunity-list expanded-list / expanded-list-name / standard-list / standard-list-name</pre> <pre>no ip extcommunity-list expanded-list / expanded-list-name / standard-list / standard-list-name</pre> <p>Cisco IOS IP Routing Protocols Command Reference (June 10, 2005), at 116.</p>	<p>ip extcommunity-list standard</p> <p>The ip extcommunity-list standard command creates an extended community list to configure Virtual Private Network (VPN) route filtering. Extended community attributes filter routes for virtual routing and forwarding instances (VRFs).</p> <ul style="list-style-type: none"> Route Target (rt) attribute identifies a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that route traffic received from corresponding sites. Site of Origin (soo) attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a specific site must be assigned the same site of origin attribute whether a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents the creation of routing loops when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed. <p>The no ip extcommunity-list standard and default ip extcommunity-list standard commands delete the specified extended community list by removing the corresponding ip extcommunity-list standard statement from <i>running-config</i>.</p> <p>Platform all Command Mode Global Configuration</p> <p>Command Syntax</p> <pre>ip extcommunity-list standard listname FILTER TYPE COMM 1 [COMM 2...COMM n]</pre> <pre>no ip extcommunity-list standard listname</pre> <pre>default ip extcommunity-list standard listname</pre> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1591.</p> <p><i>See also</i> Arista User Manual v. 4.13.6F (4/14/2014), at 1541; Arista User Manual v. 4.12.3 (7/17/13), at 1365; Arista User Manual, v. 4.11.1 (1/11/13), at 1111; Arista User Manual v. 4.10.3 (10/22/12), at 923; Arista User Manual v. 4.9.3.2 (5/3/12), at 690; Arista User Manual v. 4.8.2 (11/18/11), at 520.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<p>ip extcommunity-list</p> <p>To create an extended community list to configure Virtual Private Network (VPN) route filtering, use the ip extcommunity-list command in global configuration mode. To delete the extended community list, use the no form of this command.</p> <p>To enter IP Extended community-list configuration mode to create or configure an extended community-list, use the ip extcommunity-list command in global configuration mode. To delete the entire extended community list, use the no form of this command. To delete a single entry, use the no form in IP Extended community-list configuration mode.</p> <p>Global Configuration Mode CLI</p> <pre>ip extcommunity-list {expanded-list [permit deny] [regular-expression]} expanded list-name [permit deny] [regular-expression] standard-list [permit deny] [rt value] [soo value] standard list-name [permit deny] [rt value] [soo value]} no ip extcommunity-list {expanded-list expanded list-name standard-list standard list-name}</pre> <pre>ip extcommunity-list {expanded-list expanded list-name standard-list standard list-name} no ip extcommunity-list {expanded-list expanded list-name standard-list standard list-name}</pre> <p>Cisco IOS IP Routing: BGP Command Reference (2013), at 326.</p>	<p>ip extcommunity-list expanded</p> <p>The ip extcommunity-list expanded command creates an extended community list to configure Virtual Private Network (VPN) route filtering. Extended community attributes filter routes for virtual routing and forwarding instances (VRFs). The command uses regular expressions to name the communities specified by the list.</p> <ul style="list-style-type: none"> Route Target (rt) attribute identifies a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that route traffic received from corresponding sites. Site of Origin (soo) attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a specific site must be assigned the same site of origin attribute whether a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents the creation of routing loops when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed. <p>The no ip extcommunity-list expanded and default ip extcommunity-list expanded commands delete the specified extended community list by removing the corresponding ip community-list expanded statement from <i>running-config</i>.</p> <p>Platform all Command Mode Global Configuration</p> <p>Command Syntax</p> <pre>ip extcommunity-list expanded listname FILTER_TYPE R_EXP no ip extcommunity-list expanded listname default ip extcommunity-list expanded listname</pre> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1590.</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 1540; Arista User Manual v. 4.12.3 (7/17/13), at 1364; Arista User Manual, v. 4.11.1 (1/11/13), at 1110; Arista User Manual v. 4.10.3 (10/22/12), at 922; Arista User Manual v. 4.9.3.2 (5/3/12), at 689; Arista User Manual v. 4.8.2 (11/18/11), at 519.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 12.4</p> <p>Effective date of registration: 8/12/2005</p>	<p>ip extcommunity-list</p> <p>To create an extended community list to configure Virtual Private Network (VPN) route filtering, use the ip extcommunity-list command in global configuration mode. To delete the extended community list, use the no form of this command.</p> <p>Global Configuration Mode CLI</p> <pre>ip extcommunity-list expanded-list / expanded list-name {permit deny} [regular-expression] / standard-list / standard list-name {permit deny} [rt value] [soo value]</pre> <pre>no ip extcommunity-list expanded-list / expanded list-name standard-list / standard list-name</pre> <p>To enter IP extended community-list configuration mode to create or configure an extended community-list, use the ip extcommunity-list command in global configuration mode. To delete the entire extended community list, use the no form of this command. To delete a single entry, use the no form in IP Extended community-list configuration mode.</p> <pre>ip extcommunity-list expanded-list / expanded list-name standard-list / standard list-name</pre> <pre>no ip extcommunity-list expanded-list / expanded list-name standard-list / standard list-name</pre> <p>Cisco IOS IP Routing Protocols Command Reference (June 10, 2005), at 116.</p>	<p>ip extcommunity-list expanded</p> <p>The ip extcommunity-list expanded command creates an extended community list to configure Virtual Private Network (VPN) route filtering. Extended community attributes filter routes for virtual routing and forwarding instances (VRFs). The command uses regular expressions to name the communities specified by the list.</p> <ul style="list-style-type: none"> Route Target (rt) attribute identifies a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that route traffic received from corresponding sites. Site of Origin (soo) attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a specific site must be assigned the same site of origin attribute whether a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents the creation of routing loops when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed. <p>The no ip extcommunity-list expanded and default ip extcommunity-list expanded commands delete the specified extended community list by removing the corresponding ip community-list expanded statement from <i>running-config</i>.</p> <p>Platform all Command Mode Global Configuration</p> <p>Command Syntax</p> <pre>ip extcommunity-list expanded listname FILTER_TYPE R_EXP</pre> <pre>no ip extcommunity-list expanded listname</pre> <pre>default ip extcommunity-list expanded listname</pre> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1590.</p> <p><i>See also</i> Arista User Manual v. 4.13.6F (4/14/2014), at 1540; Arista User Manual v. 4.12.3 (7/17/13), at 1364; Arista User Manual, v. 4.11.1 (1/11/13), at 1110; Arista User Manual v. 4.10.3 (10/22/12), at 922; Arista User Manual v. 4.9.3.2 (5/3/12), at 689; Arista User Manual v. 4.8.2 (11/18/11), at 519.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<p>Route Target Extended Community Attribute</p> <p>The route target (RT) extended community attribute is configured with the <code>rt</code> keyword. This attribute is used to identify a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that are used for routing traffic that is received from corresponding sites.</p> <p>Site of Origin Extended Community Attribute</p> <p>The site of origin (SOO) extended community attribute is configured with the <code>soo</code> keyword. This attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a particular site must be assigned the same site of origin extended community attribute, regardless if a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents routing loops from occurring when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed.</p> <p>Cisco IOS IP Routing: BGP Command Reference (2013), at 330.</p>	<p>ip extcommunity-list expanded</p> <p>The <code>ip extcommunity-list expanded</code> command creates an extended community list to configure Virtual Private Network (VPN) route filtering. Extended community attributes filter routes for virtual routing and forwarding instances (VRFs). The command uses regular expressions to name the communities specified by the list.</p> <ul style="list-style-type: none"> Route Target (<code>rt</code>) attribute identifies a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that route traffic received from corresponding sites. Site of Origin (<code>soo</code>) attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a specific site must be assigned the same site of origin attribute whether a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents the creation of routing loops when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed. <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1590.</p> <p><i>See also</i> Arista User Manual v. 4.13.6F (4/14/2014), at 1540; Arista User Manual v. 4.12.3 (7/17/13), at 1364; Arista User Manual, v. 4.11.1 (1/11/13), at 1110; Arista User Manual v. 4.10.3 (10/22/12), at 922; Arista User Manual v. 4.9.3.2 (5/3/12), at 689; Arista User Manual v. 4.8.2 (11/18/11), at 519.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 12.4</p> <p>Effective date of registration: 8/12/2005</p>	<p>Route Target Extended Community Attribute</p> <p>The route target (RT) extended community attribute is configured with the rt keyword. This attribute is used to identify a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that are used for routing traffic that is received from corresponding sites.</p> <p>Site of Origin Extended Community Attribute</p> <p>The site of origin (SOO) extended community attribute is configured with the soo keyword. This attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a particular site must be assigned the same site of origin extended community attribute, regardless if a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents routing loops from occurring when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed.</p> <p>Cisco IOS IP Routing Protocols Command Reference (June 10, 2005), at 118.</p>	<p>ip extcommunity-list expanded</p> <p>The ip extcommunity-list expanded command creates an extended community list to configure Virtual Private Network (VPN) route filtering. Extended community attributes filter routes for virtual routing and forwarding instances (VRFs). The command uses regular expressions to name the communities specified by the list.</p> <ul style="list-style-type: none"> Route Target (rt) attribute identifies a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that route traffic received from corresponding sites. Site of Origin (soo) attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a specific site must be assigned the same site of origin attribute whether a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents the creation of routing loops when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed. <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1590.</p> <p><i>See also</i> Arista User Manual v. 4.13.6F (4/14/2014), at 1540; Arista User Manual v. 4.12.3 (7/17/13), at 1364; Arista User Manual, v. 4.11.1 (1/11/13), at 1110; Arista User Manual v. 4.10.3 (10/22/12), at 922; Arista User Manual v. 4.9.3.2 (5/3/12), at 689; Arista User Manual v. 4.8.2 (11/18/11), at 519.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<p>Route Target Extended Community Attribute</p> <p>The route target (RT) extended community attribute is configured with the <code>rt</code> keyword. This attribute is used to identify a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that are used for routing traffic that is received from corresponding sites.</p> <p>Site of Origin Extended Community Attribute</p> <p>The site of origin (SOO) extended community attribute is configured with the <code>soo</code> keyword. This attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a particular site must be assigned the same site of origin extended community attribute, regardless if a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents routing loops from occurring when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed.</p> <p>Cisco IOS IP Routing: BGP Command Reference (2013), at 330.</p>	<p>ip extcommunity-list standard</p> <p>The <code>ip extcommunity-list standard</code> command creates an extended community list to configure Virtual Private Network (VPN) route filtering. Extended community attributes filter routes for virtual routing and forwarding instances (VRFs).</p> <ul style="list-style-type: none"> Route Target (rt) attribute identifies a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that route traffic received from corresponding sites. Site of Origin (soo) attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a specific site must be assigned the same site of origin attribute whether a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents the creation of routing loops when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed. <p>Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1591.</p> <p><i>See also</i> Arista User Manual v. 4.13.6F (4/14/2014), at 1541; Arista User Manual v. 4.12.3 (7/17/13), at 1365; Arista User Manual, v. 4.11.1 (1/11/13), at 1111; Arista User Manual v. 4.10.3 (10/22/12), at 923; Arista User Manual v. 4.9.3.2 (5/3/12), at 690; Arista User Manual v. 4.8.2 (11/18/11), at 520.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 12.4</p> <p>Effective date of registration: 8/12/2005</p>	<p>Route Target Extended Community Attribute</p> <p>The route target (RT) extended community attribute is configured with the rt keyword. This attribute is used to identify a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that are used for routing traffic that is received from corresponding sites.</p> <p>Site of Origin Extended Community Attribute</p> <p>The site of origin (SOO) extended community attribute is configured with the soo keyword. This attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a particular site must be assigned the same site of origin extended community attribute, regardless if a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents routing loops from occurring when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed.</p> <p>Cisco IOS IP Routing Protocols Command Reference (June 10, 2005), at 118.</p>	<p>ip extcommunity-list standard</p> <p>The ip extcommunity-list standard command creates an extended community list to configure Virtual Private Network (VPN) route filtering. Extended community attributes filter routes for virtual routing and forwarding instances (VRFs).</p> <ul style="list-style-type: none"> • Route Target (rt) attribute identifies a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that route traffic received from corresponding sites. • Site of Origin (soo) attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a specific site must be assigned the same site of origin attribute whether a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents the creation of routing loops when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed. <p>Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1591.</p> <p><i>See also</i> Arista User Manual v. 4.13.6F (4/14/2014), at 1541; Arista User Manual v. 4.12.3 (7/17/13), at 1365; Arista User Manual, v. 4.11.1 (1/11/13), at 1111; Arista User Manual v. 4.10.3 (10/22/12), at 923; Arista User Manual v. 4.9.3.2 (5/3/12), at 690; Arista User Manual v. 4.8.2 (11/18/11), at 520.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<p>Route Target Extended Community Attribute</p> <p>The route target (RT) extended community attribute is configured with the <code>rt</code> keyword. This attribute is used to identify a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that are used for routing traffic that is received from corresponding sites.</p> <p>Site of Origin Extended Community Attribute</p> <p>The site of origin (SOO) extended community attribute is configured with the <code>soo</code> keyword. This attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a particular site must be assigned the same site of origin extended community attribute, regardless if a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents routing loops from occurring when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed.</p> <p>Cisco IOS IP Routing: BGP Command Reference (2013), at 330.</p>	<p>route targets (rt): This attribute identifies a set of sites and VRFs that may receive routes tagged with the configured route target. Configuring this attribute with a route allows that route to be placed in per-site forwarding tables that route traffic received from corresponding sites.</p> <p>site of origin (soo): This attribute identifies the site from where the Provider Edge (PE) router learns the route. All routes learned from a specific site have the same SOO extended community attribute, whether a site is connected to a single or multiple PE routers. This attribute prevents routing loops resulting from multihomed sites. The SOO attribute is configured on the interface and propagated into a BGP domain by redistribution. The SOO is applied to routes learned from VRFs.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1552.</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 1502; Arista User Manual v. 4.12.3 (7/17/13), at 1334; Arista User Manual, v. 4.11.1 (1/11/13), at 1083-84; Arista User Manual v. 4.10.3 (10/22/12), at 896; Arista User Manual v. 4.9.3.2 (5/3/12), at 668; Arista User Manual v. 4.8.2 (11/18/11), at 500.</p>
<p>Cisco IOS 12.4</p> <p>Effective date of registration: 8/12/2005</p>	<p>Route Target Extended Community Attribute</p> <p>The route target (RT) extended community attribute is configured with the <code>rt</code> keyword. This attribute is used to identify a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that are used for routing traffic that is received from corresponding sites.</p> <p>Site of Origin Extended Community Attribute</p> <p>The site of origin (SOO) extended community attribute is configured with the <code>soo</code> keyword. This attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a particular site must be assigned the same site of origin extended community attribute, regardless if a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents routing loops from occurring when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed.</p> <p>Cisco IOS IP Routing Protocols Command Reference (June 10, 2005), at 118.</p>	<p>route targets (rt): This attribute identifies a set of sites and VRFs that may receive routes tagged with the configured route target. Configuring this attribute with a route allows that route to be placed in per-site forwarding tables that route traffic received from corresponding sites.</p> <p>site of origin (soo): This attribute identifies the site from where the Provider Edge (PE) router learns the route. All routes learned from a specific site have the same SOO extended community attribute, whether a site is connected to a single or multiple PE routers. This attribute prevents routing loops resulting from multihomed sites. The SOO attribute is configured on the interface and propagated into a BGP domain by redistribution. The SOO is applied to routes learned from VRFs.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1552.</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 1502; Arista User Manual v. 4.12.3 (7/17/13), at 1334; Arista User Manual, v. 4.11.1 (1/11/13), at 1083-84; Arista User Manual v. 4.10.3 (10/22/12), at 896; Arista User Manual v. 4.9.3.2 (5/3/12), at 668; Arista User Manual v. 4.8.2 (11/18/11), at 500.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<p>Extended community attributes are used to configure, filter, and identify routes for virtual routing and forwarding instances (VRFs) and Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs).</p> <p>Cisco IOS IP Routing: BGP Command Reference (2013), at 359</p>	<p>BGP extended communities configure, filter, and identify routes for virtual routing, forwarding instances (VRFs), and Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs).</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/22/2014), at 1552.</p> <p><i>See also</i> Arista User Manual v. 4.13.6F (4/14/2014), at 1502; Arista User Manual v. 4.12.3 (7/17/13), at 1334; Arista User Manual, v. 4.11.1 (1/11/13), at 1083-84; Arista User Manual v. 4.10.3 (10/22/12), at 896; Arista User Manual v. 4.9.3.2 (5/3/12), at 668; Arista User Manual v. 4.8.2 (11/18/11), at 500.</p>
<p>Cisco IOS 12.4</p> <p>Effective date of registration: 8/12/2005</p>	<p>Extended community attributes are used to configure, filter, and identify routes for virtual routing and forwarding instances (VRFs) and Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs).</p> <p>Cisco IOS IP Routing Protocols Command Reference (June 10, 2005), at 135.</p>	<p>BGP extended communities configure, filter, and identify routes for virtual routing, forwarding instances (VRFs), and Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs).</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/22/2014), at 1552.</p> <p><i>See also</i> Arista User Manual v. 4.13.6F (4/14/2014), at 1502; Arista User Manual v. 4.12.3 (7/17/13), at 1334; Arista User Manual, v. 4.11.1 (1/11/13), at 1083-84; Arista User Manual v. 4.10.3 (10/22/12), at 896; Arista User Manual v. 4.9.3.2 (5/3/12), at 668; Arista User Manual v. 4.8.2 (11/18/11), at 500.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<p>neighbor ebgp-multihop</p> <p>To accept and attempt BGP connections to external peers residing on networks that are not directly connected, use the neighbor ebgp-multihop command in router configuration mode. To return to the default, use the no form of this command.</p> <p>neighbor (ip-address) (ipv6-address) peer-group-name} ebgp-multihop [ttl] no neighbor (ip-address) (ipv6-address) peer-group-name} ebgp-multihop</p> <p>Cisco IOS IP Routing: BGP Command Reference (2013), at 423.</p>	<p>neighbor ebgp-multihop</p> <p>The neighbor ebgp-multihop command programs the switch to accept and attempt BGP connections to the external peers residing on networks not directly connected to the switch. The command does not establish the multihop if the only route to the peer is the default route (0.0.0.0).</p> <p>The no neighbor ebgp-multihop command applies the system default configuration.</p> <p>The default neighbor ebgp-multihop command applies the system default configuration for individual neighbors, and applies the peer group's setting for neighbors that are members of a peer group.</p> <p>The no neighbor command removes all configuration commands for the neighbor at the specified address.</p> <p>Platform all Command Mode Router-BGP Configuration</p> <p>Command Syntax</p> <p>neighbor NEIGHBOR_ID ebgp-multihop [hop_number] no neighbor NEIGHBOR_ID ebgp-multihop default neighbor NEIGHBOR_ID ebgp-multihop</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1597.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1370; Arista User Manual, v. 4.11.1 (1/11/13), at 1116; Arista User Manual v. 4.10.3 (10/22/12), at 928; Arista User Manual v. 4.9.3.2 (5/3/12), at 693; Arista User Manual v. 4.8.2 (11/18/11), at 523; Arista User Manual v. 4.7.3 (7/18/11), at 383.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 12.4</p> <p>Effective date of registration: 8/12/2005</p>	<p>neighbor ebgp-multihop</p> <p>To accept and attempt Border Gateway Protocol (BGP) connections to external peers residing on networks that are not directly connected, use the neighbor ebgp-multihop command in router configuration mode. To return to the default, use the no form of this command.</p> <p>neighbor <i>ip-address</i> <i>peer-group-name</i> ebgp-multihop [<i>n</i>]</p> <p>no neighbor <i>ip-address</i> <i>peer-group-name</i> ebgp-multihop</p> <p>Cisco IOS IP Routing Protocols Command Reference (June 10, 2005), at 158.</p>	<p>neighbor ebgp-multihop</p> <p>The neighbor ebgp-multihop command programs the switch to accept and attempt BGP connections to the external peers residing on networks not directly connected to the switch. The command does not establish the multihop if the only route to the peer is the default route (0.0.0.0).</p> <p>The no neighbor ebgp-multihop command applies the system default configuration.</p> <p>The default neighbor ebgp-multihop command applies the system default configuration for individual neighbors, and applies the peer group's setting for neighbors that are members of a peer group.</p> <p>The no neighbor command removes all configuration commands for the neighbor at the specified address.</p> <p>Platform all Command Mode Router-BGP Configuration</p> <p>Command Syntax</p> <p>neighbor <i>NEIGHBOR_ID</i> ebgp-multihop [<i>hop_number</i>]</p> <p>no neighbor <i>NEIGHBOR_ID</i> ebgp-multihop</p> <p>default neighbor <i>NEIGHBOR_ID</i> ebgp-multihop</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1597.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1370; Arista User Manual, v. 4.11.1 (1/11/13), at 1116; Arista User Manual v. 4.10.3 (10/22/12), at 928; Arista User Manual v. 4.9.3.2 (5/3/12), at 693; Arista User Manual v. 4.8.2 (11/18/11), at 523; Arista User Manual v. 4.7.3 (7/18/11), at 383.</p>

Copyright Registration Information	Cisco	Arista		
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<div>neighbor local-as</div> <div>To customize the AS_PATH attribute for routes received from an external Border Gateway Protocol (eBGP) neighbor, or to configure the BGP—Support for iBGP Local-AS feature, use the neighbor local-as command in address family or router configuration mode. To disable AS_PATH attribute customization or iBGP Local-AS support, use the no form of this command.</div> <div>neighbor {ip-address ipv6-address peer-group-name} local-as [autonomous-system-number [no-prepend [replace-as [dual-as]]]]</div> <div>no neighbor {ip-address ipv6-address peer-group-name} local-as</div> <div>...</div> <table><tr><td>no-prepend</td><td>(Optional) Does not prepend the local autonomous system number to any routes received from the eBGP neighbor.</td></tr></table> <div>Cisco IOS IP Routing: BGP Command Reference (2013), at 442.</div>	no-prepend	(Optional) Does not prepend the local autonomous system number to any routes received from the eBGP neighbor.	<div>neighbor local-as</div> <div>The neighbor local-as command enables the modification of the AS_PATH attribute for routes received from an eBGP neighbor, allowing the switch to appear as a member of a different autonomous system (AS) to external peers. This switch does not prepend the local AS number to routes received from the eBGP neighbor. The AS number from the local BGP routing process is not prepended.</div> <div>The no neighbor local-as command disables AS_PATH modification for the specified peer or peer group.</div> <div>The default neighbor local-as command disables AS_PATH modification for individual neighbors, and applies the peer group's setting for neighbors that are members of a peer group.</div> <div>Platformall</div> <div>Command ModeRouter-BGP Configuration</div> <div>Command Syntax</div> <div>neighbor NEIGHBOR_ID local-as as id no-prepend replace-as</div> <div>no neighbor NEIGHBOR_ID local-as</div> <div>default neighbor NEIGHBOR_ID local-as</div> <div>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1601.</div> <div>See also Arista User Manual v. 4.12.3 (7/17/13), at 1373; Arista User Manual, v. 4.11.1 (1/11/13), at 1119; Arista User Manual v. 4.10.3 (10/22/12), at 931; Arista User Manual v. 4.9.3.2 (5/3/12), at 696; Arista User Manual v. 4.8.2 (11/18/11), at 526; Arista User Manual v. 4.7.3 (7/18/11), at 386.</div>
	no-prepend	(Optional) Does not prepend the local autonomous system number to any routes received from the eBGP neighbor.		

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 12.4</p> <p>Effective date of registration: 8/12/2005</p>	<p>neighbor local-as</p> <p>To customize the AS-path attribute for routes received from an external Border Gateway Protocol (eBGP) neighbor, use the neighbor local-as command in address family or router configuration mode. To disable AS-path attribute customization, use the no form of this command.</p> <p>neighbor ip-address local-as as-number [no-prepend [replace-as [dual-as]]] no neighbor ip-address local-as as-number</p> <p>...</p> <p>no-prepend (Optional) Does not prepend the local autonomous system number to any routes received from the eBGP neighbor.</p> <p>Cisco IOS IP Routing Protocols Command Reference (June 10, 2005), at 166.</p>	<p>neighbor local-as</p> <p>The neighbor local-as command enables the modification of the AS_PATH attribute for routes received from an eBGP neighbor, allowing the switch to appear as a member of a different autonomous system (AS) to external peers. This switch does not prepend the local AS number to routes received from the eBGP neighbor. The AS number from the local BGP routing process is not prepended.</p> <p>The no neighbor local-as command disables AS_PATH modification for the specified peer or peer group.</p> <p>The default neighbor local-as command disables AS_PATH modification for individual neighbors, and applies the peer group's setting for neighbors that are members of a peer group.</p> <p>Platform all Command Mode Router-BGP Configuration</p> <p>Command Syntax</p> <p>neighbor NEIGHBOR_ID local-as as id no-prepend replace-as no neighbor NEIGHBOR_ID local-as default neighbor NEIGHBOR_ID local-as</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1601.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1373; Arista User Manual, v. 4.11.1 (1/11/13), at 1119; Arista User Manual v. 4.10.3 (10/22/12), at 931; Arista User Manual v. 4.9.3.2 (5/3/12), at 696; Arista User Manual v. 4.8.2 (11/18/11), at 526; Arista User Manual v. 4.7.3 (7/18/11), at 386.</p>

Copyright Registration Information	Cisco	Arista								
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<div>neighbor remove-private-as</div> <p>To remove private autonomous system numbers from the autonomous system path (a list of autonomous systems that a route passes through to reach a BGP peer) in eBGP outbound routing updates, use the neighbor remove-private-as command in router configuration, address family configuration, or peer-group template mode. To disable this function, use the no form of this command.</p> <div>neighbor [ip-address] peer-group-name remove-private-as [all [replace-as]]</div> <div>no neighbor [ip-address] peer-group-name remove-private-as</div> <div><div>Syntax Description</div><table><tr><td>ip-address</td><td>IP address of the BGP-speaking neighbor</td></tr><tr><td>peer-group-name</td><td>Name of a BGP peer group.</td></tr><tr><td>all</td><td>(Optional) Removes all private AS numbers from the AS path in outgoing updates.</td></tr><tr><td>replace-as</td><td>(Optional) As long as the all keyword is specified, the replace-as keyword causes all private AS numbers in the AS path to be replaced with the router's local AS number.</td></tr></table></div> <div>Cisco IOS IP Routing: BGP Command Reference (2013), at 479.</div>	ip-address	IP address of the BGP-speaking neighbor	peer-group-name	Name of a BGP peer group.	all	(Optional) Removes all private AS numbers from the AS path in outgoing updates.	replace-as	(Optional) As long as the all keyword is specified, the replace-as keyword causes all private AS numbers in the AS path to be replaced with the router's local AS number.	<div>neighbor remove-private-as</div> <p>The neighbor remove-private-as command removes private autonomous system numbers from outbound routing updates for external BGP (eBGP) neighbors. When the autonomous system path includes both private and public autonomous system numbers, the REMOVAL parameter specifies how the private autonomous system number is removed.</p> <p>The no neighbor remove-private-as command applies the system default (preserves private AS numbers) for the specified peer.</p> <p>The default neighbor remove-private-as command applies the system default for individual neighbors and applies the peer group's setting for neighbors that are members of a peer group.</p> <p>The no neighbor command removes all configuration commands for the neighbor at the specified address.</p> <div><div>Platform</div><div>all</div><div>Command Mode</div><div>Router-BGP Configuration</div></div> <div>Command Syntax</div> <div>neighbor NEIGHBOR_ID remove-private-as [REMOVAL]</div> <div>no neighbor NEIGHBOR_ID remove-private-as</div> <div>default neighbor NEIGHBOR_ID remove-private-as</div> <div>Parameters</div> <div><div><div>•</div><div>NEIGHBOR_ID</div><div>IP address or peer group name. Values include:</div><div><div>—</div><div>ipv4_addr</div><div>neighbor's IPv4 address.</div></div><div><div>—</div><div>ipv6_addr</div><div>neighbor's IPv6 address.</div></div><div><div>—</div><div>group_name</div><div>peer group name.</div></div></div></div> <div><div>•</div><div>REMOVAL</div><div>Specifies removal of private autonomous AS number when path includes both private and public numbers. Values include:</div><div><div>—</div><div><no parameter></div><div>private AS numbers are not removed.</div></div><div><div>—</div><div>all</div><div>removes all private AS numbers from AS path in outbound updates.</div></div><div><div>—</div><div>all replace-as</div><div>all private AS numbers in AS path are replaced with router's local AS number.</div></div></div> <div>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1612.</div> <div>See also Arista User Manual v. 4.12.3 (7/17/13), at 1384; Arista User Manual, v. 4.11.1 (1/11/13), at 1130.</div>
	ip-address	IP address of the BGP-speaking neighbor								
	peer-group-name	Name of a BGP peer group.								
all	(Optional) Removes all private AS numbers from the AS path in outgoing updates.									
replace-as	(Optional) As long as the all keyword is specified, the replace-as keyword causes all private AS numbers in the AS path to be replaced with the router's local AS number.									

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 12.4</p> <p>Effective date of registration: 8/12/2005</p>	<p>neighbor remove-private-as</p> <p>To remove private autonomous system numbers from the autonomous system path, a list of autonomous system numbers that a route passes through to reach a BGP peer, in outbound routing updates, use the neighbor remove-private-as command in router configuration mode. To disable this function, use the no form of this command.</p> <p>neighbor {ip-address peer-group-name} remove-private-as</p> <p>no neighbor {ip-address peer-group-name} remove-private-as</p> <p>Cisco IOS IP Routing Protocols Command Reference (June 10, 2005), at 188.</p>	<p>neighbor remove-private-as</p> <p>The neighbor remove-private-as command removes private autonomous system numbers from outbound routing updates for external BGP (eBGP) neighbors. When the autonomous system path includes both private and public autonomous system numbers, the <i>REMOVAL</i> parameter specifies how the private autonomous system number is removed.</p> <p>The no neighbor remove-private-as command applies the system default (preserves private AS numbers) for the specified peer.</p> <p>The default neighbor remove-private-as command applies the system default for individual neighbors and applies the peer group's setting for neighbors that are members of a peer group.</p> <p>The no neighbor command removes all configuration commands for the neighbor at the specified address.</p> <p>Platform all Command Mode Router-BGP Configuration</p> <p>Command Syntax</p> <p>neighbor NEIGHBOR_ID remove-private-as [REMOVAL] no neighbor NEIGHBOR_ID remove-private-as default neighbor NEIGHBOR_ID remove-private-as</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1612.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1384; Arista User Manual, v. 4.11.1 (1/11/13), at 1130.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<p>neighbor route-reflector-client</p> <p>To configure the router as a BGP route reflector and configure the specified neighbor as its client, use the neighbor route-reflector-client command in address family or router configuration mode. To indicate that the neighbor is not a client, use the no form of this command.</p> <p>neighbor {ip-address ipv6-address peer-group-name} route-reflector-client no neighbor {ip-address ipv6-address peer-group-name} route-reflector-client</p> <p>Cisco IOS IP Routing: BGP Command Reference (2013), at 486</p> <p>By default, all internal BGP (iBGP) speakers in an autonomous system must be fully meshed, and neighbors do not readvertise iBGP learned routes to neighbors, thus preventing a routing information loop. When all the clients are disabled, the local router is no longer a route reflector.</p> <p>If you use route reflectors, all iBGP speakers need not be fully meshed. In the route reflector model, an Internal BGP peer is configured to be a <i>route reflector</i> responsible for passing iBGP learned routes to iBGP neighbors. This scheme eliminates the need for each router to talk to every other router.</p> <p>Use the neighbor route-reflector-client command to configure the local router as the route reflector and the specified neighbor as one of its clients. All the neighbors configured with this command will be members of the client group and the remaining iBGP peers will be members of the nonclient group for the local route reflector.</p> <p>The bgp client-to-client reflection command controls client-to-client reflection.</p> <p>Cisco IOS IP Routing: BGP Command Reference (2013), at 487.</p>	<p>neighbor route-reflector-client</p> <p>Participating BGP routers within an AS communicate EBGP-learned routes to all of their peers, but to prevent routing loops they must not re-advertise iBGP-learned routes within the AS. To ensure that all members of the AS share the same routing information, a fully meshed network topology (in which each member router of the AS is connected to every other member) can be used, but this topology can result in high volumes of iBGP messages when it is scaled. Instead, in larger networks one or more routers can be configured as route reflectors.</p> <p>A route reflector is configured to re-advertise routes learned through iBGP to a group of BGP neighbors within the AS (its clients), eliminating the need for a fully meshed topology.</p> <p>The neighbor route-reflector-client command configures the switch to act as a route reflector and configures the specified neighbor as one of its clients. Additional clients can be specified by re-issuing the command.</p> <p>The bgp client-to-client reflection command controls client-to-client reflection.</p> <p>The no neighbor route-reflector-client and default neighbor route-reflector-client commands disable route reflection by deleting the neighbor route-reflector-client command from <i>running-config</i>.</p> <p>Platform all Command Mode Router-BGP Configuration</p> <p>Command Syntax</p> <p>neighbor NEIGHBOR_ID route-reflector-client no neighbor NEIGHBOR_ID route-reflector-client default neighbor NEIGHBOR_ID route-reflector-client</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1614.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1386; Arista User Manual, v. 4.11.1 (1/11/13), at 1132.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 12.4</p> <p>Effective date of registration: 8/12/2005</p>	<p>neighbor route-reflector-client</p> <p>To configure the router as a BGP route reflector and configure the specified neighbor as its client, use the neighbor route-reflector-client command in address family or router configuration mode. To indicate that the neighbor is not a client, use the no form of this command.</p> <p>neighbor <i>ip-address</i> route-reflector-client</p> <p>no neighbor <i>ip-address</i> route-reflector-client</p> <p>Usage Guidelines</p> <p>By default, all internal BGP (iBGP) speakers in an autonomous system must be fully meshed, and neighbors do not readvertise iBGP learned routes to neighbors, thus preventing a routing information loop. When all the clients are disabled, the local router is no longer a route reflector.</p> <p>If you use route reflectors, all iBGP speakers need not be fully meshed. In the route reflector model, an interior BGP peer is configured to be a <i>route reflector</i> responsible for passing iBGP learned routes to iBGP neighbors. This scheme eliminates the need for each router to talk to every other router.</p> <p>Use the neighbor route-reflector-client command to configure the local router as the route reflector and the specified neighbor as one of its clients. All the neighbors configured with this command will be members of the client group and the remaining iBGP peers will be members of the nonclient group for the local route reflector.</p> <p>The bgp client-to-client reflection command controls client-to-client reflection.</p> <p>Cisco IOS IP Routing Protocols Command Reference (June 10, 2005), at 192.</p>	<p>neighbor route-reflector-client</p> <p>Participating BGP routers within an AS communicate EBGP-learned routes to all of their peers, but to prevent routing loops they must not re-advertise iBGP-learned routes within the AS. To ensure that all members of the AS share the same routing information, a fully meshed network topology (in which each member router of the AS is connected to every other member) can be used, but this topology can result in high volumes of iBGP messages when it is scaled. Instead, in larger networks one or more routers can be configured as route reflectors.</p> <p>A route reflector is configured to re-advertise routes learned through iBGP to a group of BGP neighbors within the AS (its clients), eliminating the need for a fully meshed topology.</p> <p>The neighbor route-reflector-client command configures the switch to act as a route reflector and configures the specified neighbor as one of its clients. Additional clients can be specified by re-issuing the command.</p> <p>The bgp client-to-client reflection command controls client-to-client reflection.</p> <p>The no neighbor route-reflector-client and default neighbor route-reflector-client commands disable route reflection by deleting the neighbor route-reflector-client command from <i>running-config</i>.</p> <p>Platform all</p> <p>Command Mode Router-BGP Configuration</p> <p>Command Syntax</p> <p>neighbor <i>NEIGHBOR_ID</i> route-reflector-client</p> <p>no neighbor <i>NEIGHBOR_ID</i> route-reflector-client</p> <p>default neighbor <i>NEIGHBOR_ID</i> route-reflector-client</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1614.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1386; Arista User Manual, v. 4.11.1 (1/11/13), at 1132.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<div data-bbox="304 280 1115 375"> <div data-bbox="304 280 709 375">neighbor ebgp-multihop</div> <div data-bbox="709 280 1115 375">Accepts and attempts BGP connections to external peers residing on networks that are not directly connected.</div> </div> <p>Cisco IOS IP Routing: BGP Command Reference (2013), at 416.</p>	<div data-bbox="1171 280 2051 410"> <div data-bbox="1171 280 1493 313">neighbor ebgp-multihop</div> <div data-bbox="1171 337 2051 410">The neighbor ebgp-multihop command programs the switch to accept and attempt BGP connections to the external peers residing on networks not directly connected to the switch. The command does not establish the multihop if the only route to the peer is the default route (0.0.0.0).</div> </div> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1597.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1370; Arista User Manual, v. 4.11.1 (1/11/13), at 1116; Arista User Manual v. 4.10.3 (10/22/12), at 928; Arista User Manual v. 4.9.3.2 (5/3/12), at 693; Arista User Manual v. 4.8.2 (11/18/11), at 523; Arista User Manual v. 4.7.3 (7/18/11), at 383.</p>
<p>Cisco IOS 12.4</p> <p>Effective date of registration: 8/12/2005</p>	<div data-bbox="304 711 1115 764"> <div data-bbox="304 711 506 764">neighbor ebgp-multihop</div> <div data-bbox="506 711 1115 764">Accepts and attempts BGP connections to external peers residing on networks that are not directly connected.</div> </div> <p>Cisco IOS IP Routing Protocols Command Reference (June 10, 2005), at 173.</p>	<div data-bbox="1171 711 2051 846"> <div data-bbox="1171 711 1493 743">neighbor ebgp-multihop</div> <div data-bbox="1171 768 2051 846">The neighbor ebgp-multihop command programs the switch to accept and attempt BGP connections to the external peers residing on networks not directly connected to the switch. The command does not establish the multihop if the only route to the peer is the default route (0.0.0.0).</div> </div> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1597.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1370; Arista User Manual, v. 4.11.1 (1/11/13), at 1116; Arista User Manual v. 4.10.3 (10/22/12), at 928; Arista User Manual v. 4.9.3.2 (5/3/12), at 693; Arista User Manual v. 4.8.2 (11/18/11), at 523; Arista User Manual v. 4.7.3 (7/18/11), at 383.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<div data-bbox="310 284 1129 329"> <div>neighbor route-map</div> <div>Applies a route map to inbound or outbound routes</div> </div> <p>Cisco IOS IP Routing: BGP Command Reference (2013), at 524.</p>	<p>neighbor route-map (BGP)</p> <p>The neighbor route-map command applies a route map to inbound or outbound BGP routes. When a route map is applied to outbound routes, the switch will advertise only routes matching at least one section of the route map. Only one outbound route map and one inbound route map can be applied to a given neighbor. A new route map applied to a neighbor will replace the previous route map.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1613.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1385; Arista User Manual, v. 4.11.1 (1/11/13), at 1131; Arista User Manual v. 4.10.3 (10/22/12), at 943.</p>
<p>Cisco IOS 12.4</p> <p>Effective date of registration: 8/12/2005</p>	<div data-bbox="310 673 1129 719"> <div>neighbor route-map</div> <div>Applies a route map to inbound or outbound routes</div> </div> <p>Cisco IOS IP Routing Protocols Command Reference (June 10, 2005), at 204.</p>	<p>neighbor route-map (BGP)</p> <p>The neighbor route-map command applies a route map to inbound or outbound BGP routes. When a route map is applied to outbound routes, the switch will advertise only routes matching at least one section of the route map. Only one outbound route map and one inbound route map can be applied to a given neighbor. A new route map applied to a neighbor will replace the previous route map.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1613.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1385; Arista User Manual, v. 4.11.1 (1/11/13), at 1131; Arista User Manual v. 4.10.3 (10/22/12), at 943.</p>

Copyright Registration Information	Cisco	Arista																						
	<div><div>show ip bgp ipv4 multicast summary</div><div>To display a summary of IP Version 4 multicast database-related information, use the show ip bgp ipv4 multicast summary command in EXEC mode.</div><div>show ip bgp ipv4 multicast summary</div></div> <div>Cisco IOS IP Routing: BGP Command Reference (2013), at 757</div> <div>Table 54: show ip bgp ipv4 multicast summary Field Descriptions</div> <table><tr><th>Field</th><th>Description</th></tr><tr><td>Neighbor</td><td>IP address of configured neighbor in the multicast routing table.</td></tr><tr><td>V</td><td>Version of multiprotocol BGP used.</td></tr><tr><td>AS</td><td>Autonomous system to which the neighbor belongs.</td></tr><tr><td>MsgRcvd</td><td>Number of messages received from the neighbor.</td></tr><tr><td>MsgSent</td><td>Number of messages sent to the neighbor.</td></tr><tr><td>TblVer</td><td>Number of the table version, which is incremented each time the table changes.</td></tr><tr><td>InQ</td><td>Number of messages received in the input queue.</td></tr><tr><td>OutQ</td><td>Number of messages ready to go in the output queue.</td></tr><tr><td>Up/Down</td><td>Days and hours that the neighbor has been up or down (no information in the State column means the connection is up).</td></tr><tr><td>State/PfxRcd</td><td>State of the neighbor/number of routes received. If no state is indicated, the state is up.</td></tr></table>	Field	Description	Neighbor	IP address of configured neighbor in the multicast routing table.	V	Version of multiprotocol BGP used.	AS	Autonomous system to which the neighbor belongs.	MsgRcvd	Number of messages received from the neighbor.	MsgSent	Number of messages sent to the neighbor.	TblVer	Number of the table version, which is incremented each time the table changes.	InQ	Number of messages received in the input queue.	OutQ	Number of messages ready to go in the output queue.	Up/Down	Days and hours that the neighbor has been up or down (no information in the State column means the connection is up).	State/PfxRcd	State of the neighbor/number of routes received. If no state is indicated, the state is up.	<div><div>show ip bgp summary</div><div>The show ip bgp summary command displays BGP path, prefix, and attribute information for all BGP neighbors.</div><div>Platformall Command ModeEXEC</div><div>Command Syntax</div><div>show ip bgp summary [VRF_INSTANCE]</div><div>Parameters</div><div><div><div>VRF_INSTANCE</div>specifies VRF instances.</div><div><div><no parameter></div>displays routing table for context-active VRE.</div><div><div>vrf vrf_name</div>displays routing table for the specified VRE.</div><div><div>vrf all</div>displays routing table for all VRFs.</div><div><div>vrf default</div>displays routing table for default VRF.</div></div><div>Display Values</div><div>Header Row</div><div><div>BGP router identifier:</div>The router identifier – loopback address or highest IP address.</div><div><div>Local AS Number:</div>AS number assigned to switch</div><div>Neighbor Table Columns</div><div><div>(First) Neighbor:</div>IP address of the neighbor.</div><div><div>(Second) V:</div>BGP version number spoken to the neighbor</div><div><div>(Third) AS:</div>Neighbor's Autonomous system number.</div><div><div>(Fourth) MsgRcvd:</div>Number of messages received from the neighbor.</div><div><div>(Fifth) MsgSent:</div>Number of messages sent to the neighbor.</div><div><div>(Sixth) InQ:</div>Number of messages queued to be processed from the neighbor.</div><div><div>(Seventh) OutQ:</div>Number of messages queued to be sent to the neighbor.</div><div><div>(Eighth) Up/Down:</div>Period the BGP session has been in Established state or its current status.</div><div><div>(Ninth) State:</div>State of the BGP session and the number of routes received from a neighbor.</div></div> <div>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1641.</div> <div>See also Arista User Manual v. 4.12.3 (7/17/13), at 1407; Arista User Manual, v. 4.11.1 (1/11/13), at 1153; Arista User Manual v. 4.10.3 (10/22/12), at 964; Arista User Manual v. 4.9.3.2 (5/3/12), at 728; Arista User Manual v. 4.8.2 (11/18/11), at 549; Arista User Manual v. 4.7.3 (7/18/11), at 402.</div>
Field	Description																							
Neighbor	IP address of configured neighbor in the multicast routing table.																							
V	Version of multiprotocol BGP used.																							
AS	Autonomous system to which the neighbor belongs.																							
MsgRcvd	Number of messages received from the neighbor.																							
MsgSent	Number of messages sent to the neighbor.																							
TblVer	Number of the table version, which is incremented each time the table changes.																							
InQ	Number of messages received in the input queue.																							
OutQ	Number of messages ready to go in the output queue.																							
Up/Down	Days and hours that the neighbor has been up or down (no information in the State column means the connection is up).																							
State/PfxRcd	State of the neighbor/number of routes received. If no state is indicated, the state is up.																							

Copyright Registration Information	Cisco	Arista																						
Cisco IOS 12.4 Effective date of registration: 8/12/2005	<div>show ip bgp ipv4 multicast summary</div> <p>To display a summary of IP Version 4 multicast database-related information, use the <code>show ip bgp ipv4 multicast summary</code> command in EXEC mode.</p> <div>show ip bgp ipv4 multicast summary</div> <table><caption>Table 27 show ip bgp ipv4 multicast summary Field Descriptions</caption><thead><tr><th>Field</th><th>Description</th></tr></thead><tbody><tr><td>Neighbor</td><td>IP address of configured neighbor in the multicast routing table.</td></tr><tr><td>V</td><td>Version of multiprotocol BGP used.</td></tr><tr><td>AS</td><td>Autonomous system to which the neighbor belongs.</td></tr><tr><td>MsgRcvd</td><td>Number of messages received from the neighbor.</td></tr><tr><td>MsgSent</td><td>Number of messages sent to the neighbor.</td></tr><tr><td>TblVer</td><td>Number of the table version, which is incremented each time the table changes.</td></tr><tr><td>InQ</td><td>Number of messages received in the input queue.</td></tr><tr><td>OutQ</td><td>Number of messages ready to go in the output queue.</td></tr><tr><td>Up/Down</td><td>Days and hours that the neighbor has been up or down (no information in the State column means the connection is up).</td></tr><tr><td>State/PfxRcd</td><td>State of the neighbor/number of routes received. If no state is indicated, the state is up.</td></tr></tbody></table> <p>Cisco IOS IP Routing Protocols Command Reference (June 10, 2005), at 308.</p>	Field	Description	Neighbor	IP address of configured neighbor in the multicast routing table.	V	Version of multiprotocol BGP used.	AS	Autonomous system to which the neighbor belongs.	MsgRcvd	Number of messages received from the neighbor.	MsgSent	Number of messages sent to the neighbor.	TblVer	Number of the table version, which is incremented each time the table changes.	InQ	Number of messages received in the input queue.	OutQ	Number of messages ready to go in the output queue.	Up/Down	Days and hours that the neighbor has been up or down (no information in the State column means the connection is up).	State/PfxRcd	State of the neighbor/number of routes received. If no state is indicated, the state is up.	<div>show ip bgp summary</div> <p>The <code>show ip bgp summary</code> command displays BGP path, prefix, and attribute information for all BGP neighbors.</p> <div>Platformall Command ModeEXEC</div> <p>Command Syntax</p> <div>show ip bgp summary [VRF_INSTANCE]</div> <p>Parameters</p> <ul style="list-style-type: none">VRF_INSTANCE specifies VRF instances.<ul style="list-style-type: none"><no parameter> displays routing table for context-active VRE.vrf vrf_name displays routing table for the specified VRF.vrf all displays routing table for all VRFs.vrf default displays routing table for default VRF. <p>Display Values</p> <p>Header Row</p> <ul style="list-style-type: none">BGP router identifier: The router identifier – loopback address or highest IP address.Local AS Number: AS number assigned to switch <p>Neighbor Table Columns</p> <ul style="list-style-type: none">(First) Neighbor: IP address of the neighbor.(Second) V: BGP version number spoken to the neighbor(Third) AS: Neighbor's Autonomous system number.(Fourth) MsgRcvd: Number of messages received from the neighbor.(Fifth) MsgSent: Number of messages sent to the neighbor.(Sixth) InQ: Number of messages queued to be processed from the neighbor.(Seventh) OutQ: Number of messages queued to be sent to the neighbor.(Eighth) Up/Down: Period the BGP session has been in Established state or its current status.(Ninth) State: State of the BGP session and the number of routes received from a neighbor. <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1641.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1407; Arista User Manual, v. 4.11.1 (1/11/13), at 1153; Arista User Manual v. 4.10.3 (10/22/12), at 964; Arista User Manual v. 4.9.3.2 (5/3/12), at 728; Arista User Manual v. 4.8.2 (11/18/11), at 549; Arista User Manual v. 4.7.3 (7/18/11), at 402.</p>
	Field	Description																						
	Neighbor	IP address of configured neighbor in the multicast routing table.																						
V	Version of multiprotocol BGP used.																							
AS	Autonomous system to which the neighbor belongs.																							
MsgRcvd	Number of messages received from the neighbor.																							
MsgSent	Number of messages sent to the neighbor.																							
TblVer	Number of the table version, which is incremented each time the table changes.																							
InQ	Number of messages received in the input queue.																							
OutQ	Number of messages ready to go in the output queue.																							
Up/Down	Days and hours that the neighbor has been up or down (no information in the State column means the connection is up).																							
State/PfxRcd	State of the neighbor/number of routes received. If no state is indicated, the state is up.																							

Copyright Registration Information	Cisco	Arista												
<div>Cisco IOS 15.4</div> <div>Effective date of registration: 11/26/2014</div>	<p>The following is sample output from the <code>show ip bgp paths</code> command in privileged EXEC mode:</p> <pre>Router# show ip bgp paths Address Hash Refcount Metric Path 0x60E5742C 0 1 0 1 0x60E3D7AC 2 1 0 ? 0x60E5C6C0 11 3 0 10 ? 0x60E577B0 35 2 40 10 ?</pre> <p>The table below describes the significant fields shown in the display.</p> <p><i>Table 64: show ip bgp paths Field Descriptions</i></p> <table><tr><th>Field</th><th>Description</th></tr><tr><td>Address</td><td>Internal address where the path is stored.</td></tr><tr><td>Hash</td><td>Hash bucket where path is stored.</td></tr><tr><td>Refcount</td><td>Number of routes using that path.</td></tr><tr><td>Metric</td><td>The Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)</td></tr><tr><td>Path</td><td>The autonomous system path for that route, followed by the origin code for that route.</td></tr></table> <p>Cisco IOS IP Routing: BGP Command Reference (2013), at 795.</p>	Field	Description	Address	Internal address where the path is stored.	Hash	Hash bucket where path is stored.	Refcount	Number of routes using that path.	Metric	The Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)	Path	The autonomous system path for that route, followed by the origin code for that route.	<p>show ip bgp paths</p> <p>The show ip bgp paths command displays all BGP paths in the database.</p> <p>Platform all Command Mode EXEC</p> <p>Command Syntax</p> <p><code>show ip bgp paths [VRF_INSTANCE]</code></p> <p>Parameters</p> <ul style="list-style-type: none"><code>VRF_INSTANCE</code> specifies VRF instances.<ul style="list-style-type: none"><code><no parameter></code> displays routing table for context-active VRF.<code>vrf vrf_name</code> displays routing table for the specified VRF.<code>vrf all</code> displays routing table for all VRFs.<code>vrf default</code> displays routing table for default VRF. <p>Display Values</p> <ul style="list-style-type: none">Refcount: Number of routes using a listed path.Metric: The Multi Exit Discriminator (MED) metric for the path.Path: The autonomous system path for that route, followed by the origin code for that route. <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1638,</p> <p><i>See also</i> Arista User Manual v. 4.13.6F (4/14/2014), at 1588; Arista User Manual v. 4.12.3 (7/17/13), at 1405; Arista User Manual, v. 4.11.1 (1/11/13), at 1151; Arista User Manual v. 4.10.3 (10/22/12), at 962; Arista User Manual v. 4.9.3.2 (5/3/12), at 725; Arista User Manual v. 4.8.2 at 547; Arista User Manual v. 4.8.2 (11/18/11), at 547; Arista User Manual v. 4.7.3 (7/18/11), at 401; Arista User Manual v. 4.6.0 (12/22/2010), at 249; Arista User Manual v. 4.6.0 (12/22/2010), at 249</p>
	Field	Description												
	Address	Internal address where the path is stored.												
	Hash	Hash bucket where path is stored.												
	Refcount	Number of routes using that path.												
Metric	The Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)													
Path	The autonomous system path for that route, followed by the origin code for that route.													

Copyright Registration Information	Cisco	Arista												
Cisco IOS 12.4 Effective date of registration: 8/12/2005	<p>The following is sample output from the show ip bgp paths command in privileged EXEC mode:</p> <pre>Router# show ip bgp paths Address Hash Refcount Metric Path 0x6085742C 0 1 0 1 0x6085742C 2 1 0 7 0x6085742C 11 3 0 10 3 0x6085742C 35 2 40 10 7</pre> <p>Table 33 describes the significant fields shown in the display.</p> <p>Table 33 show ip bgp paths Field Descriptions</p> <table><tr><th>Field</th><th>Description</th></tr><tr><td>Address</td><td>Internal address where the path is stored.</td></tr><tr><td>Hash</td><td>Hash bucket where path is stored.</td></tr><tr><td>Refcount</td><td>Number of routes using that path.</td></tr><tr><td>Metric</td><td>The Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)</td></tr><tr><td>Path</td><td>The autonomous system path for that route, followed by the origin code for that route.</td></tr></table> <p>Cisco IOS IP Routing Protocols Command Reference (June 10, 2005), at 308.</p>	Field	Description	Address	Internal address where the path is stored.	Hash	Hash bucket where path is stored.	Refcount	Number of routes using that path.	Metric	The Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)	Path	The autonomous system path for that route, followed by the origin code for that route.	<p>show ip bgp paths</p> <p>The show ip bgp paths command displays all BGP paths in the database.</p> <p>Platform all Command Mode EXEC</p> <p>Command Syntax</p> <p>show ip bgp paths [VRF_INSTANCE]</p> <p>Parameters</p> <ul style="list-style-type: none">VRF_INSTANCE specifies VRF instances.<ul style="list-style-type: none"><no parameter> displays routing table for context-active VRF.vrf vrf_name displays routing table for the specified VRF.vrf all displays routing table for all VRFs.vrf default displays routing table for default VRF. <p>Display Values</p> <ul style="list-style-type: none">Refcount: Number of routes using a listed path.Metric: The Multi Exit Discriminator (MED) metric for the path.Path: The autonomous system path for that route, followed by the origin code for that route. <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1638,</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 1588; Arista User Manual v. 4.12.3 (7/17/13), at 1405; Arista User Manual, v. 4.11.1 (1/11/13), at 1151; Arista User Manual v. 4.10.3 (10/22/12), at 962; Arista User Manual v. 4.9.3.2 (5/3/12), at 725; Arista User Manual v. 4.8.2 at 547; Arista User Manual v. 4.8.2 (11/18/11), at 547; Arista User Manual v. 4.7.3 (7/18/11), at 401; Arista User Manual v. 4.6.0 (12/22/2010), at 249; Arista User Manual v. 4.6.0 (12/22/2010), at 249</p>
	Field	Description												
Address	Internal address where the path is stored.													
Hash	Hash bucket where path is stored.													
Refcount	Number of routes using that path.													
Metric	The Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)													
Path	The autonomous system path for that route, followed by the origin code for that route.													

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<p data-bbox="306 280 1136 329">The <code>show ip bgp summary</code> command is used to display BGP path, prefix, and attribute information for all connections to BGP neighbors.</p> <p data-bbox="306 367 1062 399">Cisco IOS IP Routing: BGP Command Reference (2013), at 819.</p>	<p data-bbox="1178 280 1472 313">show ip bgp summary</p> <p data-bbox="1178 334 2051 383">The <code>show ip bgp summary</code> command displays BGP path, prefix, and attribute information for all BGP neighbors.</p> <p data-bbox="1178 420 1881 453">Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1641.</p> <p data-bbox="1178 490 2028 652"><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1407; Arista User Manual, v. 4.11.1 (1/11/13), at 1153; Arista User Manual v. 4.10.3 (10/22/12), at 964; Arista User Manual v. 4.9.3.2 (5/3/12), at 728; Arista User Manual v. 4.8.2 (11/18/11), at 549; Arista User Manual v. 4.7.3 (7/18/11), at 402.</p>
Cisco IOS 12.4 Effective date of registration: 8/12/2005	<p data-bbox="306 699 1136 748">The <code>show ip bgp summary</code> command is used to display BGP path, prefix, and attribute information for all connections to BGP neighbors.</p> <p data-bbox="306 786 1125 850">Cisco IOS IP Routing Protocols Command Reference (July 16, 2005), at 323.</p>	<p data-bbox="1178 691 1472 724">show ip bgp summary</p> <p data-bbox="1178 745 2051 794">The <code>show ip bgp summary</code> command displays BGP path, prefix, and attribute information for all BGP neighbors.</p> <p data-bbox="1178 831 1881 863">Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1641.</p> <p data-bbox="1178 901 2028 1063"><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1407; Arista User Manual, v. 4.11.1 (1/11/13), at 1153; Arista User Manual v. 4.10.3 (10/22/12), at 964; Arista User Manual v. 4.9.3.2 (5/3/12), at 728; Arista User Manual v. 4.8.2 (11/18/11), at 549; Arista User Manual v. 4.7.3 (7/18/11), at 402.</p>

Copyright Registration Information	Cisco	Arista				
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<table><tr><td>Up/Down</td><td>The length of time that the BGP session has been in the Established state, or the current status if not in the Established state.</td></tr></table> <p>Cisco IOS IP Routing: BGP Command Reference (2013), at 821.</p> <table><tr><td>State/PfxRcd</td><td>Current state of the BGP session, and the number of prefixes that have been received from a neighbor or peer group. When the maximum number (as set by the neighbor maximum-prefix command) is reached, the string "PfxRcd" appears in the entry, the neighbor is shut down, and the connection is set to Idle. An (Admin) entry with Idle status indicates that the connection has been shut down using the neighbor shutdown command.</td></tr></table> <p>Cisco IOS IP Routing: BGP Command Reference (2013), at 822.</p>	Up/Down	The length of time that the BGP session has been in the Established state, or the current status if not in the Established state.	State/PfxRcd	Current state of the BGP session, and the number of prefixes that have been received from a neighbor or peer group. When the maximum number (as set by the neighbor maximum-prefix command) is reached, the string "PfxRcd" appears in the entry, the neighbor is shut down, and the connection is set to Idle. An (Admin) entry with Idle status indicates that the connection has been shut down using the neighbor shutdown command.	<p>Neighbor Table Columns</p> <ul style="list-style-type: none">• (First) Neighbor: IP address of the neighbor.• (Second) V: BGP version number spoken to the neighbor• (Third) AS: Neighbor's Autonomous system number.• (Fourth) MsgRcvd: Number of messages received from the neighbor.• (Fifth) MsgSent: Number of messages sent to the neighbor.• (Sixth) InQ: Number of messages queued to be processed from the neighbor.• (Seventh) OutQ: Number of messages queued to be sent to the neighbor.• (Eighth) Up/Down: Period the BGP session has been in Established state or its current status.• (Ninth) State: State of the BGP session and the number of routes received from a neighbor. <p>After the maximum number of routes are received (maximum paths (BGP)), the field displays PfxRcd, the neighbor is shut down, and the connection is set to Idle.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1641.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1407; Arista User Manual, v. 4.11.1 (1/11/13), at 1153; Arista User Manual v. 4.10.3 (10/22/12), at 964; Arista User Manual v. 4.9.3.2 (5/3/12), at 728.</p>
Up/Down	The length of time that the BGP session has been in the Established state, or the current status if not in the Established state.					
State/PfxRcd	Current state of the BGP session, and the number of prefixes that have been received from a neighbor or peer group. When the maximum number (as set by the neighbor maximum-prefix command) is reached, the string "PfxRcd" appears in the entry, the neighbor is shut down, and the connection is set to Idle. An (Admin) entry with Idle status indicates that the connection has been shut down using the neighbor shutdown command.					
Cisco IOS 12.4 Effective date of registration: 8/12/2005	<table><tr><td>Up/Down</td><td>The length of time that the BGP session has been in the Established state, or the current state if it is not Established.</td></tr><tr><td>State/PfxRcd</td><td>Current state of the BGP session/the number of prefixes the router has received from a neighbor or peer group. When the maximum number (as set by the neighbor maximum-prefix command) is reached, the string "PfxRcd" appears in the entry, the neighbor is shut down, and the connection is Idle. An (Admin) entry with Idle status indicates that the connection has been shut down using the neighbor shutdown command.</td></tr></table> <p>Cisco IOS IP Routing Protocols Command Reference (June 10, 2005), at 318.</p>	Up/Down	The length of time that the BGP session has been in the Established state, or the current state if it is not Established.	State/PfxRcd	Current state of the BGP session/the number of prefixes the router has received from a neighbor or peer group. When the maximum number (as set by the neighbor maximum-prefix command) is reached, the string "PfxRcd" appears in the entry, the neighbor is shut down, and the connection is Idle. An (Admin) entry with Idle status indicates that the connection has been shut down using the neighbor shutdown command.	<p>Neighbor Table Columns</p> <ul style="list-style-type: none">• (First) Neighbor: IP address of the neighbor.• (Second) V: BGP version number spoken to the neighbor• (Third) AS: Neighbor's Autonomous system number.• (Fourth) MsgRcvd: Number of messages received from the neighbor.• (Fifth) MsgSent: Number of messages sent to the neighbor.• (Sixth) InQ: Number of messages queued to be processed from the neighbor.• (Seventh) OutQ: Number of messages queued to be sent to the neighbor.• (Eighth) Up/Down: Period the BGP session has been in Established state or its current status.• (Ninth) State: State of the BGP session and the number of routes received from a neighbor. <p>After the maximum number of routes are received (maximum paths (BGP)), the field displays PfxRcd, the neighbor is shut down, and the connection is set to Idle.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1641.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1407; Arista User Manual, v. 4.11.1 (1/11/13), at 1153; Arista User Manual v. 4.10.3 (10/22/12), at 964; Arista User Manual v. 4.9.3.2 (5/3/12), at 728.</p>
Up/Down	The length of time that the BGP session has been in the Established state, or the current state if it is not Established.					
State/PfxRcd	Current state of the BGP session/the number of prefixes the router has received from a neighbor or peer group. When the maximum number (as set by the neighbor maximum-prefix command) is reached, the string "PfxRcd" appears in the entry, the neighbor is shut down, and the connection is Idle. An (Admin) entry with Idle status indicates that the connection has been shut down using the neighbor shutdown command.					

Copyright Registration Information	Cisco	Arista												
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<div>bfd</div> <p>To set the baseline Bidirectional Forwarding Detection (BFD) session parameters on an interface, use the bfd command in interface configuration mode. To remove the baseline BFD session parameters, use the no bfd command.</p> <div>bfd interval milliseconds min_rx milliseconds multiplier multiplier-value no bfd interval milliseconds min_rx milliseconds multiplier multiplier-value</div> <div><table><tr><td>Syntax Description</td><td><table><tr><td>interval milliseconds</td><td>Specifies the rate, in milliseconds, at which BFD control packets will be sent to BFD peers. The valid range for the <i>milliseconds</i> argument is from 50 to 999.</td></tr><tr><td>min_rx milliseconds</td><td>Specifies the rate, in milliseconds, at which BFD control packets will be expected to be received from BFD peers. The valid range for the <i>milliseconds</i> argument is from 50 to 999.</td></tr><tr><td>multiplier multiplier-value</td><td>Specifies the number of consecutive BFD control packets that must be missed from a BFD peer before BFD declares that the peer is unavailable and the Layer 3 BFD peer is informed of the failure. The valid range for the <i>multiplier-value</i> argument is from 3 to 50.</td></tr></table></td></tr></table></div> <div>Cisco IOS IP Routing: Protocol-Independent Command Reference (2013), at 9</div>	Syntax Description	<table><tr><td>interval milliseconds</td><td>Specifies the rate, in milliseconds, at which BFD control packets will be sent to BFD peers. The valid range for the <i>milliseconds</i> argument is from 50 to 999.</td></tr><tr><td>min_rx milliseconds</td><td>Specifies the rate, in milliseconds, at which BFD control packets will be expected to be received from BFD peers. The valid range for the <i>milliseconds</i> argument is from 50 to 999.</td></tr><tr><td>multiplier multiplier-value</td><td>Specifies the number of consecutive BFD control packets that must be missed from a BFD peer before BFD declares that the peer is unavailable and the Layer 3 BFD peer is informed of the failure. The valid range for the <i>multiplier-value</i> argument is from 3 to 50.</td></tr></table>	interval milliseconds	Specifies the rate, in milliseconds, at which BFD control packets will be sent to BFD peers. The valid range for the <i>milliseconds</i> argument is from 50 to 999.	min_rx milliseconds	Specifies the rate, in milliseconds, at which BFD control packets will be expected to be received from BFD peers. The valid range for the <i>milliseconds</i> argument is from 50 to 999.	multiplier multiplier-value	Specifies the number of consecutive BFD control packets that must be missed from a BFD peer before BFD declares that the peer is unavailable and the Layer 3 BFD peer is informed of the failure. The valid range for the <i>multiplier-value</i> argument is from 3 to 50.	<div>bfd</div> <p>The bfd command configures BFD parameters for the configuration mode interface. All BFD sessions that pass through this interface will use these parameters. If custom parameters are not configured, the interface will use default values for BFD sessions passing through it.</p> <p>For a BFD session to be established, BFD must be enabled for any routing protocol using BFD for failure detection.</p> <p>The no bfd and default bfd commands return the BFD parameters on the configuration mode interface to default values by removing the corresponding bfd command from <i>running-config</i>.</p> <div><table><tr><td>Platform</td><td>all</td></tr><tr><td>Command Mode</td><td>Interface-Ethernet Configuration Interface-Loopback Configuration Interface-Management Configuration Interface-Port-channel Configuration Interface-VLAN Configuration</td></tr></table></div> <div>Command Syntax</div> <div>bfd interval transmit_rate min_rx receive_minimum multiplier factor no bfd default bfd</div> <div>Parameters</div> <div><ul style="list-style-type: none">transmit_rate specifies the rate in milliseconds at which BFD control packets will be sent to BFD peers. Values range from 50 to 60000; the default value is 300.receive_minimum specifies the rate in milliseconds at which BFD control packets will be expected from BFD peers. Values range from 50 to 60000.factor specifies the number of consecutive missed BFD control packets from a BFD peer that will designate the peer as unavailable and indicate failure to the Layer 3 BFD peer. Values range from 3 to 50.</div> <div>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1741.</div> <div>See also Arista User Manual v. 4.12.3 (7/17/13), at 1471.</div>	Platform	all	Command Mode	Interface-Ethernet Configuration Interface-Loopback Configuration Interface-Management Configuration Interface-Port-channel Configuration Interface-VLAN Configuration
	Syntax Description	<table><tr><td>interval milliseconds</td><td>Specifies the rate, in milliseconds, at which BFD control packets will be sent to BFD peers. The valid range for the <i>milliseconds</i> argument is from 50 to 999.</td></tr><tr><td>min_rx milliseconds</td><td>Specifies the rate, in milliseconds, at which BFD control packets will be expected to be received from BFD peers. The valid range for the <i>milliseconds</i> argument is from 50 to 999.</td></tr><tr><td>multiplier multiplier-value</td><td>Specifies the number of consecutive BFD control packets that must be missed from a BFD peer before BFD declares that the peer is unavailable and the Layer 3 BFD peer is informed of the failure. The valid range for the <i>multiplier-value</i> argument is from 3 to 50.</td></tr></table>	interval milliseconds	Specifies the rate, in milliseconds, at which BFD control packets will be sent to BFD peers. The valid range for the <i>milliseconds</i> argument is from 50 to 999.	min_rx milliseconds	Specifies the rate, in milliseconds, at which BFD control packets will be expected to be received from BFD peers. The valid range for the <i>milliseconds</i> argument is from 50 to 999.	multiplier multiplier-value	Specifies the number of consecutive BFD control packets that must be missed from a BFD peer before BFD declares that the peer is unavailable and the Layer 3 BFD peer is informed of the failure. The valid range for the <i>multiplier-value</i> argument is from 3 to 50.						
	interval milliseconds	Specifies the rate, in milliseconds, at which BFD control packets will be sent to BFD peers. The valid range for the <i>milliseconds</i> argument is from 50 to 999.												
min_rx milliseconds	Specifies the rate, in milliseconds, at which BFD control packets will be expected to be received from BFD peers. The valid range for the <i>milliseconds</i> argument is from 50 to 999.													
multiplier multiplier-value	Specifies the number of consecutive BFD control packets that must be missed from a BFD peer before BFD declares that the peer is unavailable and the Layer 3 BFD peer is informed of the failure. The valid range for the <i>multiplier-value</i> argument is from 3 to 50.													
Platform	all													
Command Mode	Interface-Ethernet Configuration Interface-Loopback Configuration Interface-Management Configuration Interface-Port-channel Configuration Interface-VLAN Configuration													

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<p>ip route</p> <p>To establish static routes, use the <code>ip route</code> command in global configuration mode. To remove static routes, use the <code>no</code> form of this command.</p> <p><code>ip route</code> [vrf vrf-name] prefix mask {ip-address} interface-type interface-number [ip-address] [dhcp] [global] [distance] [multicast] [name next-hop-name] [permanent] track number [tag tag]</p> <p><code>no ip route</code> [vrf vrf-name] prefix mask {ip-address} interface-type interface-number [ip-address] [dhcp] [global] [distance] multicast [name next-hop-name] [permanent] track number [tag tag]</p> <p>Cisco IOS IP Routing: Protocol-Independent Command Reference (2013), at 62</p> <p>If you specify an administrative distance, you are flagging a static route that can be overridden by dynamic information. For example, routes derived with Enhanced Interior Gateway Routing Protocol (EIGRP) have a default administrative distance of 100. To have a static route that would be overridden by an EIGRP dynamic route, specify an administrative distance greater than 100. Static routes have a default administrative distance of 1.</p> <p>Cisco IOS IP Routing: Protocol-Independent Command Reference (2013), at 63</p>	<p>ip route</p> <p>The <code>ip route</code> command creates a static route. The destination is a network segment; the next-hop address is either an IPv4 address or a routable port. When multiple routes exist to a destination prefix, the route with the lowest administrative distance takes precedence.</p> <p>Static routes have a default administrative distance of 1. Assigning a higher administrative distance to a static route configures it to be overridden by dynamic routing data. For example, a static route with a distance value of 200 is overridden by OSPF intra-area routes with a default distance of 110.</p> <p>...</p> <p>Command Syntax</p> <p><code>ip route</code> [VRF_INSTANCE] dest_net NEXT_HOP [DISTANCE] [TAG_OPTION] [RT_NAME]</p> <p><code>no ip route</code> [VRF_INSTANCE] dest_net [NEXT_HOP] [DISTANCE]</p> <p><code>default ip route</code> [VRF_INSTANCE] dest_net [NEXT_HOP] [DISTANCE]</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1287.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1082; Arista User Manual, v. 4.11.1 (1/11/13), at 860; Arista User Manual v. 4.10.3 (10/22/12), at 683.</p>
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<p>show ipv6 route summary</p> <p>Displays the current contents of the IPv6 routing table in summary format.</p> <p>Cisco IOS IP Routing: Protocol-Independent Command Reference (2013), at 284</p>	<p>show ipv6 route summary</p> <p>The <code>show ipv6 route summary</code> command displays the current contents of the IPv6 routing table in summary format.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1337.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1165.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<p>Usage Guidelines Learn lists are a way to categorize learned traffic classes. In each learn list, different criteria for learning traffic classes including prefixes, application definitions, filters, and aggregation parameters can be configured. A traffic class is automatically learned by PIR based on each learn list criteria, and each learn list is configured with a sequence number. The sequence number determines the order in which learn list criteria are applied. Learn lists allow different PIR policies to be applied to each learn list; in previous releases the traffic classes could not be divided, and a PIR policy was applied to all the traffic classes profiled during one learning session.</p> <p>Cisco IOS Performance Routing Command Reference (2010), at 131.</p>	<p>Route maps define conditions for redistributing routes between routing protocols. A route map clause is identified by a name, filter type (permit or deny) and sequence number. Clauses with the same name are components of a single route map; the sequence number determines the order in which the clauses are compared to a route.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 894.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 773; Arista User Manual, v. 4.11.1 (1/11/13), at 602; Arista User Manual v. 4.10.3 (10/22/12), at 516; Arista User Manual v. 4.9.3.2 (5/3/12), at 439; Arista User Manual v. 4.8.2 (11/18/11), at 316.</p>
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<p>Usage Guidelines The set interface command is entered on a master controller in PIR map configuration mode. This command can be used for PIR black hole filtering if the border routers detect a denial-of-service (DoS) attack by directing packets to the null interface. The null interface is a virtual network interface that is similar to the loopback interface. Whereas traffic to the loopback interface is directed to the router itself, traffic sent to the null interface is discarded. This interface is always up and can never forward or receive traffic; encapsulation always fails. The null interface functions similarly to the null devices available on most operating systems. Null interfaces are used as a low-overhead method of discarding unnecessary network traffic.</p> <p>Cisco IOS Performance Routing Command Reference (2010), at 226.</p>	<p>14.4.6 Null0 Interface</p> <p>The null0 interface is a virtual interface that drops all inbound packets. A null0 route is a network route whose destination is null0 interface. Inbound packets to a null0 interface are not forwarded to any valid address. Many interface configuration commands provide null0 as an interface option.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 633.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 502; Arista User Manual, v. 4.11.1 (1/11/13), at 397; Arista User Manual v. 4.10.3 (10/22/12), at 329.</p>

Copyright Registration Information	Cisco	Arista						
<div>Cisco IOS 15.4</div> <div>Effective date of registration: 11/26/2014</div>	<div><div>snmp-server enable traps pfr</div><div>To enable Performance Routing (PFR) Simple Network Management Protocol (SNMP) notifications (traps and informs), use the <code>snmp-server enable traps pfr</code> command in global configuration mode. To disable PFR notifications, use the <code>no</code> form of this command</div><div><div>snmp-server enable traps pfr</div><div>no snmp-server enable traps pfr</div></div><div><div>Syntax Description</div><div>This command has no arguments or keywords.</div></div><div><div>Command Default</div><div>PFR SNMP notifications are disabled.</div></div><div><div>Command Modes</div><div>Global configuration (config)</div></div><div><div>Command History</div><table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>Cisco IOS XE Release 3.7S</td><td>This command was introduced.</td></tr><tr><td>15.3(2)T</td><td>This command was integrated into Cisco IOS Release 15.3(2)T.</td></tr></tbody></table></div><div><div>Usage Guidelines</div><div>Use this command to enable SNMP notifications for PFR activity</div></div><div><div>Examples</div><div><div>This example shows how to enable PFR SNMP notifications:</div><div>Router(config)# snmp-server host 10.2.2.2 traps public pfr Router(config)# snmp-server enable traps pfr Router(config)# exit</div></div></div><div>Cisco IOS Performance Routing Command Reference (2010), at 372.</div></div>	Release	Modification	Cisco IOS XE Release 3.7S	This command was introduced.	15.3(2)T	This command was integrated into Cisco IOS Release 15.3(2)T.	<div><div>snmp-server enable traps</div><div>The <code>snmp-server enable traps</code> command enables the transmission of Simple Network Management Protocol (SNMP) notifications as traps or inform requests. This command enables both traps and inform requests for the specified notification types. The <code>snmp-server host</code> command specifies the notification type (traps or informs). Sending notifications requires at least one <code>snmp-server host</code> command.</div><div>The <code>snmp-server enable traps</code> and <code>no snmp-server enable traps</code> commands, without an MIB parameter, specifies the default notification trap generation setting for all MIBs. These commands, when specifying an MIB, controls notification generation for the specified MIB. The default <code>snmp-server enable traps</code> command resets notification generation to the default setting for the specified MIB.</div><div><div>Platform</div><div>all</div><div>Command Mode</div><div>Global Configuration</div></div><div><div>Command Syntax</div><div><div>snmp-server enable traps [trap_type]</div><div>no snmp-server enable traps [trap_type]</div><div>default snmp-server enable traps [trap_type]</div></div></div><div><div>Parameters</div><div><ul style="list-style-type: none"><code>trap_type</code> controls the generation of informs or traps for the specified MIB:<ul style="list-style-type: none"><code><no parameter></code> controls notifications for MIBs not covered by specific commands.<code>entity</code> controls entity-MIB modification notifications.<code>lldp</code> controls LLDP notifications.<code>msdpBackwardTransition</code> controls msdpBackwardTransition notifications.<code>msdpEstablished</code> controls msdpEstablished notifications.<code>snmp</code> controls SNMP-v2 notifications.<code>switchover</code> controls switchover notifications.<code>snmpConfigManEvent</code> controls snmpConfigManEvent notifications.<code>test</code> controls test traps.</div></div><div><div>Examples</div><div><ul style="list-style-type: none">These commands enables notification generation for all MIBs except spanning tree.<div>switch(config)#snmp-server enable traps switch(config)#no snmp-server enable traps spanning-tree switch(config)#</div>This command enables spanning-tree MIB notification generation, regardless of the default setting.<div>switch(config)#snmp-server enable traps spanning-tree switch(config)#</div></div></div><div>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1990.</div><div>See also Arista User Manual v. 4.12.3 (7/17/13), at 1680; Arista User Manual, v. 4.11.1 (1/11/13), at 1365; Arista User Manual v. 4.10.3 (10/22/12), at 1132; Arista User Manual v. 4.9.3.2 (5/3/12), at 888; Arista</div></div>
	Release	Modification						
Cisco IOS XE Release 3.7S	This command was introduced.							
15.3(2)T	This command was integrated into Cisco IOS Release 15.3(2)T.							

Copyright Registration Information	Cisco	Arista				
		User Manual v. 4.8.2 (11/18/11), at 696; Arista User Manual v. 4.7.3 (7/18/11), at 552.				
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<div><div>no snmp-server</div><div>To disable Simple Network Management Protocol (SNMP) agent operation, use the no snmp-server command in global configuration mode.</div><div>no snmp-server</div><div><div>Syntax Description</div><div>This command has no arguments or keywords.</div></div><div><div>Command Default</div><div>No default behavior or values.</div></div><div><div>Command Modes</div><div>Global configuration</div></div><div><div>Command History</div><table><tr><th>Release</th><th>Modification</th></tr><tr><td>10.0</td><td>This command was introduced.</td></tr></table></div><div><div>Usage Guidelines</div><div>This command disables all running versions of SNMP (SNMPv1, SNMPv2C, and SNMPv3) on the device.</div></div><div><div>Examples</div><div>The following example disables the current running version of SNMP:</div><div>Routed(config)# no snmp-server</div></div><div>Cisco IOS SNMP Support Command Reference (2013), at 52.</div></div>	Release	Modification	10.0	This command was introduced.	<div><div>no snmp-server</div><div>The no snmp-server and default snmp-server commands disable Simple Network Management Protocol (SNMP) agent operation by removing all snmp-server commands from running-config. SNMP is enabled with any snmp-server community or snmp-server user command.</div><div><div>Platform</div><div>all</div></div><div><div>Command Mode</div><div>Global Configuration</div></div><div><div>Command Syntax</div><div>no snmp-server</div><div>default snmp-server</div></div><div><div>Example</div><div><ul style="list-style-type: none">This command disables SNMP agent operation on the switch<div>switch(config)#no snmp-server</div><div>switch(config)#</div></div></div><div>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1973.</div><div>See also Arista User Manual v. 4.12.3 (7/17/13), at 1663; Arista User Manual, v. 4.11.1 (1/11/13), at 1350; Arista User Manual v. 4.10.3 (10/22/12), at 1117; Arista User Manual v. 4.9.3.2 (5/3/12), at 873; Arista User Manual v. 4.8.2 (11/18/11), at 681; Arista User Manual v. 4.7.3 (7/18/11), at 537.</div></div>
	Release	Modification				
10.0	This command was introduced.					

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<p>Examples</p> <p>The following is sample output from the <code>show snmp</code> command:</p> <pre> Router# show snmp Chassis: 12161083 0 SNMP packets input 0 Bad SNMP version errors 0 Unknown community name 0 Illegal operation for community name supplied 0 Encoding errors 0 Number of requested variables 0 Number of altered variables 0 Get-request PDUs 0 Get-next PDUs 0 Set-request PDUs 0 Input queue packet drops (Maximum queue size 1000) 0 SNMP packets output 0 Too big errors (Maximum packet size 1500) 0 No such name errors 0 Bad values errors 0 General errors 0 Response PDUs 0 Trap PDUs SNMP logging: enabled SNMP trap Queue: 0 dropped due to resource failure. </pre> <p>Cisco IOS SNMP Support Command Reference (2013), at 83.</p>	<p>Example</p> <ul style="list-style-type: none"> This command configures <code>xyz-1234</code> as the chassis-ID string, then displays the result. <pre> switch(config)#snmp-server chassis-id xyz-1234 switch(config)#show snmp Chassis: xyz-1234 <---chassis ID </pre> <pre> 8 SNMP packets input 0 Bad SNMP version errors 0 Unknown community name 0 Illegal operation for community name supplied 0 Encoding errors 8 Number of requested variables 0 Number of altered variables 4 Get-request PDUs 4 Get-next PDUs 0 Set-request PDUs 21 SNMP packets output 0 Too big errors 0 No such name errors 0 Bad value errors 0 General errors 8 Response PDUs 0 Trap PDUs SNMP logging: enabled Logging to taccon.162 SNMP agent enabled switch(config)# </pre> <p>Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1967-68.</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 1896; Arista User Manual v. 4.12.3 (7/17/13), at 1658; Arista User Manual, v. 4.11.1 (1/11/13), at 1344-45; Arista User Manual v. 4.10.3 (10/22/12), at 1111; Arista User Manual v. 4.9.3.2 (5/3/12), at 867; Arista User Manual v. 4.8.2 (11/18/11), at 678; Arista User Manual v. 4.7.3 (7/18/11), at 534.</p>

Copyright Registration Information	Cisco	Arista								
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<div>show snmp engineID</div> <div>To display the identification of the local Simple Network Management Protocol (SNMP) engine and all remote engines that have been configured on the router, use the <code>show snmp engineID</code> command in EXEC mode.</div> <div>show snmp engineID</div> <div>Syntax Description This command has no arguments or keywords.</div> <div>Command Modes EXEC</div> <div>Command History<table><tr><th>Release</th><th>Modification</th></tr><tr><td>12.0(3)T</td><td>This command was introduced.</td></tr><tr><td>12.2(33)SRA</td><td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td></tr><tr><td>12.2SX</td><td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td></tr></table></div> <div>Usage Guidelines An SNMP engine is a copy of SNMP that can reside on a local or remote device.</div> <div>Examples<p>The following example specifies 0000000902000000C025808 as the local engineID and 123456789ABCDEF00000000 as the remote engine ID, 172.16.37.61 as the IP address of the remote engine (copy of SNMP) and 162 as the port from which the remote device is connected to the local device:</p><pre>Router# show snmp engineID Local SNMP engineID: 0000000902000000C025808 Remote Engine ID IP-addr Port 123456789ABCDEF00000000 172.16.37.61 162</pre><p>The table below describes the fields shown in the display.</p></div> <div>Cisco IOS SNMP Support Command Reference (2013), at 91.</div>	Release	Modification	12.0(3)T	This command was introduced.	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.	<div>show snmp engineID</div> <div>The <code>show snmp engineID</code> command displays the identification of the local Simple Network Management Protocol (SNMP) engine and of all remote engines that are configured on the switch.</div> <div>Platform all</div> <div>Command Mode EXEC</div> <div>Command Syntax<div>show snmp engineID</div></div> <div>Example<ul style="list-style-type: none">This command displays the ID of the local SNMP engine.<pre>switch> show snmp engineid Local SNMP EngineID: f5717f001c730436d700 switch></pre><div>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1978.</div><div>See also Arista User Manual v. 4.12.3 (7/17/13), at 1668; Arista User Manual, v. 4.11.1 (1/11/13), at 1355; Arista User Manual v. 4.10.3 (10/22/12), at 1122; Arista User Manual v. 4.9.3.2 (5/3/12), at 878; Arista User Manual v. 4.8.2 (11/18/11), at 686; Arista User Manual v. 4.7.3 (7/18/11), at 542.</div></div>
	Release	Modification								
12.0(3)T	This command was introduced.									
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.									
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.									

Copyright Registration Information	Cisco	Arista				
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<div>Related Commands</div> <table><thead><tr><th>Command</th><th>Description</th></tr></thead><tbody><tr><td>snmp-server engineID local</td><td>Configures a name for either the local or remote SNMP engine on the router.</td></tr></tbody></table> <p>Cisco IOS SNMP Support Command Reference (2013), at 92.</p>	Command	Description	snmp-server engineID local	Configures a name for either the local or remote SNMP engine on the router.	<p>Configuring the Engine ID</p> <p>The snmp-server engineID remote command configures the name for the local or remote Simple Network Management Protocol (SNMP) engine. An SNMP engine ID is a name for the local or remote SNMP engine.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1966.</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 1894; Arista User Manual v. 4.12.3 (7/17/13), at 1656; Arista User Manual, v. 4.11.1 (1/11/13), at 1343; Arista User Manual v. 4.10.3 (10/22/12), at 1109; Arista User Manual v. 4.9.3.2 (5/3/12), at 865; Arista User Manual v. 4.8.2 (11/18/11), at 676; Arista User Manual v. 4.7.3 (7/18/11), at 432.</p>
	Command	Description				
snmp-server engineID local	Configures a name for either the local or remote SNMP engine on the router.					
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<table><tbody><tr><td>security model</td><td>The security model used by the group, either v1, v2c, or v3.</td></tr></tbody></table> <p>Cisco IOS SNMP Support Command Reference (2013), at 92.</p>	security model	The security model used by the group, either v1, v2c, or v3.	<ul style="list-style-type: none">• VERSION the security model used by the group.<ul style="list-style-type: none">— v1 SNMPv1. Uses a community string match for authentication.— v2c SNMPv2c. Uses a community string match for authentication.— v3 no auth SNMPv3. Uses a username match for authentication.— v3 auth SNMPv3. HMAC-MD5 or HMAC-SHA authentication.— v3 priv SNMPv3. HMAC-MD5 or HMAC-SHA authentication. AES or DES encryption. <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1994.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1684; Arista User Manual, v. 4.11.1 (1/11/13), at 1369; Arista User Manual v. 4.10.3 (10/22/12), at 1136; Arista User Manual v. 4.9.3.2 (5/3/12), at 892; Arista User Manual v. 4.8.2 (11/18/11), at 699; Arista User Manual v. 4.7.3 (7/18/11), at 555.</p>		
security model	The security model used by the group, either v1, v2c, or v3.					

Copyright Registration Information	Cisco	Arista																												
<div>Cisco IOS 15.4</div> <div>Effective date of registration: 11/26/2014</div>	<div><div>show snmp host</div><div>To display the recipient details for Simple Network Management Protocol (SNMP) notification operations, use the <code>show snmp host</code> command in privileged EXEC mode.</div><div><div>show snmp host</div></div><div><div>Syntax Description</div><div>This command has no arguments or keywords.</div></div><div><div>Command Default</div><div>The information configured for SNMP notification operation is displayed.</div></div><div><div>Command Modes</div><div>Privileged EXEC (#)</div></div><div><div>Command History</div><table><tr><th>Release</th><th>Modification</th></tr><tr><td>12.4(12)T</td><td>This command was introduced.</td></tr><tr><td>12.2(31)SB</td><td>This command was integrated into Cisco IOS Release 12.2(31)SB2.</td></tr><tr><td>12.2SX</td><td>This command was integrated into Cisco IOS Release 12.2SX.</td></tr></table></div><div><div>Usage Guidelines</div><div>The <code>show snmp host</code> command displays details such as IP address of the Network Management System (NMS), notification type, SNMP version, and the port number of the NMS. To configure these details, use the <code>snmp-server host</code> command.</div></div><div><div>Examples</div><div>The following is sample output from the <code>show snmp host</code> command: <pre>Router#show snmp host Notification host: 10.2.22.20 udp-port: 162 type: inform user: public security model: v2c traps: 00000000.00000000.00000000</pre><div>The table below describes the significant fields shown in the display.</div><div><div>Table 5: show snmp host Field Descriptions</div><table><tr><th>Field</th><th>Description</th></tr><tr><td>Notification host</td><td>Displays the IP address of the host for which the notification is generated.</td></tr><tr><td>udp-port</td><td>Displays the port number.</td></tr><tr><td>type</td><td>Displays the type of notification.</td></tr></table><table><tr><th>Field</th><th>Description</th></tr><tr><td>user</td><td>Displays the access type of the user for which the notification is generated.</td></tr><tr><td>security model</td><td>Displays the SNMP version used to send notifications.</td></tr><tr><td>traps</td><td>Displays details of the notification generated.</td></tr></table></div></div><div><div>Related Commands</div><table><tr><th>Command</th><th>Description</th></tr><tr><td>snmp-server host</td><td>Configures the recipient details for SNMP notification operations.</td></tr></table></div></div></div>	Release	Modification	12.4(12)T	This command was introduced.	12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB2.	12.2SX	This command was integrated into Cisco IOS Release 12.2SX.	Field	Description	Notification host	Displays the IP address of the host for which the notification is generated.	udp-port	Displays the port number.	type	Displays the type of notification.	Field	Description	user	Displays the access type of the user for which the notification is generated.	security model	Displays the SNMP version used to send notifications.	traps	Displays details of the notification generated.	Command	Description	snmp-server host	Configures the recipient details for SNMP notification operations.	<div><div>show snmp host</div><div>The <code>show snmp host</code> command displays the recipient details for Simple Network Management Protocol (SNMP) notification operations. Details that the command displays include IP address and port number of the Network Management System (NMS), notification type, and SNMP version.</div><div><div>Platform</div><div>all</div></div><div><div>Command Mode</div><div>EXEC</div></div><div><div>Command Syntax</div><div><div>show snmp host</div></div></div><div><div>Field Descriptions</div><ul style="list-style-type: none"><div>Notification host</div> IP address of the host for which the notification is generated.<div>udp-port</div> port number.<div>type</div> notification type.<div>user</div> access type of the user for which the notification is generated.<div>security model</div> SNMP version used to send notifications.<div>traps</div> details of the notification generated.</div><div><div>Example</div><ul style="list-style-type: none">This command displays the hosts configured on the switch.<div><div>switch#show snmp host</div><div>Notification host: 172.22.22.20 udp-port: 162 type: trap</div><div>user: public security model: v2c</div><div>switch></div></div></div></div>
	Release	Modification																												
12.4(12)T	This command was introduced.																													
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB2.																													
12.2SX	This command was integrated into Cisco IOS Release 12.2SX.																													
Field	Description																													
Notification host	Displays the IP address of the host for which the notification is generated.																													
udp-port	Displays the port number.																													
type	Displays the type of notification.																													
Field	Description																													
user	Displays the access type of the user for which the notification is generated.																													
security model	Displays the SNMP version used to send notifications.																													
traps	Displays details of the notification generated.																													
Command	Description																													
snmp-server host	Configures the recipient details for SNMP notification operations.																													

Copyright Registration Information	Cisco	Arista								
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<p>show snmp location</p> <p>To display the Simple Network Management Protocol (SNMP) system location string, use the show snmp location command in privileged EXEC mode.</p> <p>show snmp location</p> <p>Syntax Description This command has no arguments or keywords.</p> <p>Command Default The SNMP system location information is displayed.</p> <p>Command Modes Privileged EXEC (#)</p> <p>Command History</p> <table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>12.4(12)T</td><td>This command was introduced.</td></tr><tr><td>12.2(31)SB</td><td>This command was integrated into Cisco IOS Release 12.2(31)SB2.</td></tr><tr><td>12.2SX</td><td>This command was integrated into Cisco IOS Release 12.2SX.</td></tr></tbody></table> <p>Usage Guidelines To configure system location details, use the snmp-server location command.</p> <p>Cisco IOS SNMP Support Command Reference (2013), at 97.</p>	Release	Modification	12.4(12)T	This command was introduced.	12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB2.	12.2SX	This command was integrated into Cisco IOS Release 12.2SX.	<p>show snmp location</p> <p>The show snmp location command displays the Simple Network Management Protocol (SNMP) system location string. The snmp-server location command configures system location details. The command has no effect if a location string was not previously configured.</p> <p>Platform all Command Mode EXEC</p> <p>Command Syntax</p> <p>show snmp location</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1980.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1671; Arista User Manual, v. 4.11.1 (1/11/13), at 1358; Arista User Manual v. 4.10.3 (10/22/12), at 1125; Arista User Manual v. 4.9.3.2 (5/3/12), at 881; Arista User Manual v. 4.8.2 (11/18/11), at 689; Arista User Manual v. 4.7.3 (7/18/11), at 545.</p>
	Release	Modification								
12.4(12)T	This command was introduced.									
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB2.									
12.2SX	This command was integrated into Cisco IOS Release 12.2SX.									
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<p>SNMP management information is viewed as a collection of managed objects, residing in a virtual information store, termed the Management Information Base (MIB). Collections of related objects are defined in MIB modules. These modules are written using a subset of OSI's Abstract Syntax Notation One (ASN.1), termed the Structure of Management Information (SMI).</p> <p>Cisco IOS SNMP Support Command Reference (2013), at 98..</p>	<ul style="list-style-type: none">Management Information Base (MIB): The MIB stores network management information, which consists of collections of managed objects. Within the MIB are collections of related objects, defined in MIB modules. <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1961.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1651; Arista User Manual, v. 4.11.1 (1/11/13), at 1339; Arista User Manual v. 4.10.3 (10/22/12), at 1105; Arista User Manual v. 4.9.3.2 (5/3/12), at 861; Arista User Manual v. 4.8.2 (11/18/11), at 673; Arista User Manual v. 4.7.3 (7/18/11), at 529.</p>								

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<p>show snmp group</p> <p>Displays the names of configured SNMP groups, the security model being used, the status of the different views, and the storage type of each group.</p> <p>Cisco IOS SNMP Support Command Reference (2013), at 123.</p>	<p>show snmp group</p> <p>The show snmp group command displays the names of configured SNMP groups along with the security model, and view status of each group.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1971</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1669; Arista User Manual, v. 4.11.1 (1/11/13), at 1356; Arista User Manual v. 4.10.3 (10/22/12), at 1123; Arista User Manual v. 4.9.3.2 (5/3/12), at 879; Arista User Manual v. 4.8.2 (11/18/11), at 687; Arista User Manual v. 4.7.3 (7/18/11), at 543.</p>
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<p>show snmp view</p> <p>Displays the family name, storage type, and status of an SNMP configuration and associated MIB.</p> <p>Cisco IOS SNMP Support Command Reference (2013), at 123.</p>	<p>show snmp view</p> <p>The show snmp view command displays the family name, storage type, and status of a Simple Network Management Protocol (SNMP) configuration and the associated MIB. SNMP views are configured with the <code>snmp-server view</code> command.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1986.</p> <p><i>See also</i> Arista User Manual v. 4.13.6F (4/14/2014), at 1914; Arista User Manual v. 4.12.3 (7/17/13), at 1676; Arista User Manual, v. 4.11.1 (1/11/13), at 1361; Arista User Manual v. 4.10.3 (10/22/12), at 1128; Arista User Manual v. 4.9.3.2 (5/3/12), at 884; Arista User Manual v. 4.8.2 (11/18/11), at 692; Arista User Manual v. 4.7.3 (7/18/11), at 548.</p>

Copyright Registration Information	Cisco	Arista						
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<table><tr><td>snmp-server group</td><td>Configures a new SNMP group or a table that maps SNMP users to SNMP views.</td></tr><tr><td>snmp-server trap authentication vrf</td><td>Controls VRF-specific SNMP authentication failure notifications.</td></tr><tr><td>snmp-server user</td><td>Configures a new user to an SNMP group.</td></tr></table>	snmp-server group	Configures a new SNMP group or a table that maps SNMP users to SNMP views.	snmp-server trap authentication vrf	Controls VRF-specific SNMP authentication failure notifications.	snmp-server user	Configures a new user to an SNMP group.	<p>Configuring the Group</p> <p>An SNMP group is a table that maps SNMP users to SNMP views. The <code>snmp-server group</code> command configures a new SNMP group.</p> <p>Example</p> <ul style="list-style-type: none">This command configures <i>normal_one</i> as an SNMPv3 group (authentication and encryption) that provides access to the <i>all-items</i> read view. <pre>switch(config)#snmp-server group normal_one v3 priv read all-items switch(config)#</pre> <p>Configuring the User</p> <p>An SNMP user is a member of an SNMP group. The <code>snmp-server user</code> command adds a new user to an SNMP group and configures that user's parameters. To configure a remote user, specify the IP address or port number of the device where the user's remote SNMP agent resides.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1966.</p> <p><i>See also</i> Arista User Manual v. 4.13.6F (4/14/2014), at 1894; Arista User Manual v. 4.12.3 (7/17/13), at 1656; Arista User Manual, v. 4.11.1 (1/11/13), at 1343-44; Arista User Manual v. 4.10.3 (10/22/12), at 1109-10; Arista User Manual v. 4.9.3.2 (5/3/12), at 865; Arista User Manual v. 4.8.2 (11/18/11), at 677; Arista User Manual v. 4.7.3 (7/18/11), at 533.</p>
	snmp-server group	Configures a new SNMP group or a table that maps SNMP users to SNMP views.						
	snmp-server trap authentication vrf	Controls VRF-specific SNMP authentication failure notifications.						
snmp-server user	Configures a new user to an SNMP group.							

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<p>snmp trap link-status</p> <p>To enable Simple Network Management Protocol (SNMP) link trap generation, use the snmp trap link-status command in either interface configuration mode or service instance configuration mode. To disable SNMP link trap generation, use the no form of this command.</p> <p>snmp trap link-status [permit duplicates] no snmp trap link-status [permit duplicates]</p> <p>Cisco IOS SNMP Support Command Reference (2013), at 130.</p>	<p>snmp trap link-status</p> <p>The snmp trap link-status command enables Simple Network Management Protocol (SNMP) link-status trap generation on the configuration mode interface. The generation of link-status traps is enabled by default. If SNMP link-trap generation was previously disabled, this command removes the corresponding no snmp link-status statement from the configuration to re-enable link-trap generation.</p> <p>The no snmp trap link-status command disables SNMP link trap generation on the configuration mode interface.</p> <p>The snmp trap link-status and default snmp trap link-status commands restore the default behavior by removing the no snmp trap link-status command from <i>running-config</i>. Only the no form of this command is visible in <i>running-config</i>.</p> <p>Platform all Command Mode Interface-Ethernet Configuration Interface-Loopback Configuration Interface-Management Configuration Interface-Port-channel Configuration Interface-VLAN Configuration Interface-VXLAN Configuration</p> <p>Command Syntax</p> <p>snmp trap link-status no snmp trap link-status default snmp trap link-status</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1966.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1692; Arista User Manual, v. 4.11.1 (1/11/13), at 1377; Arista User Manual v. 4.10.3 (10/22/12), at 1144; Arista User Manual v. 4.9.3.2 (5/3/12), at 898; Arista User Manual v. 4.8.2 (11/18/11), at 705; Arista User Manual v. 4.7.3 (7/18/11), at 561.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<p><code>snmp-server host</code> Specifies the targeted recipient of an SNMP notification operation.</p> <p>Cisco IOS SNMP Support Command Reference (2013), at 191.</p>	<p>Configuring the Host</p> <p>The <code>snmp-server host</code> command specifies the recipient of a SNMP notification. An SNMP host is the recipient of an SNMP trap operation. The <code>snmp-server host</code> command sets the community string if it was not previously configured.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1967.</p> <p><i>See also</i> Arista User Manual v. 4.13.6F (4/14/2014), at 1895; Arista User Manual v. 4.12.3 (7/17/13), at 1656; Arista User Manual, v. 4.11.1 (1/11/13), at 1344; Arista User Manual v. 4.10.3 (10/22/12), at 1110; Arista User Manual v. 4.9.3.2 (5/3/12), at 866; Arista User Manual v. 4.8.2 (11/18/11), at 677; Arista User Manual v. 4.7.3 (7/18/11), at 533.</p>
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<p>Usage Guidelines <code>SNMP notifications</code> can be sent as traps or inform requests. This command enables both traps and inform requests.</p> <p>Cisco IOS SNMP Support Command Reference (2013), at 216.</p>	<p>The <code>snmp-server enable traps</code> command enables the transmission of Simple Network Management Protocol (SNMP) notifications as traps or inform requests. This command enables both traps and inform requests for the specified notification types. The <code>snmp-server host</code> command specifies the notification type (traps or informs). Sending notifications requires at least one <code>snmp-server host</code> command.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1990.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1680; Arista User Manual, v. 4.11.1 (1/11/13), at 1365; Arista User Manual v. 4.10.3 (10/22/12), at 1132; Arista User Manual v. 4.9.3.2 (5/3/12), at 888; Arista User Manual v. 4.8.2 at 696; Arista User Manual v. 4.7.3 (7/18/11), at 552.</p>

Copyright Registration Information	Cisco	Arista								
	<div><div>snmp-server engineID local</div><div>To specify the Simple Network Management Protocol (SNMP) engine ID on the local device, use the <code>snmp-server engineID local</code> command in global configuration mode. To remove the configured engine ID, use the no form of this command.</div><div><div>snmp-server engineID local engineID-string</div><div>no snmp-server engineID local engineID-string</div></div><div><div>Syntax Description</div><div><div>engineID-string</div><div>String of a maximum of 24 characters that identifies the engine ID.</div></div></div><div><div>Command Default</div><div>An SNMP engine ID is generated automatically but is not displayed or stored in the running configuration. You can display the default or configured engine ID by using the <code>show snmp engineID</code> command.</div></div><div><div>Command Modes</div><div>Global configuration (config)</div></div><div><div>Command History</div><div><table><tr><th>Release</th><th>Modification</th></tr><tr><td>12.0(3)T</td><td>This command was introduced.</td></tr><tr><td>12.2(33)SRA</td><td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td></tr><tr><td>12.2SX</td><td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td></tr></table></div></div><div><div>Usage Guidelines</div><div><p>The SNMP engine ID is a unique string used to identify the device for administrative purposes. You do not need to specify an engine ID for the device; a default string is generated using Cisco's enterprise number (1.3.6.1.4.1.9) and the MAC address of the first interface on the device. For further details on the SNMP engine ID, see RFC 2571.</p><p>If you specify your own ID, note that the entire 24-character engine ID is not needed if it contains trailing zeros. Specify only the portion of the engine ID up until the point where only zeros remain in the value. For example, to configure an engine ID of 123400000000000000000000, you can specify <code>snmp-server engineID local 1234</code>.</p><p>The value for the engine ID is displayed in hexadecimal value pairs. If the length of the input is an odd number, the last digit will be prepended with a zero ("0"). For example, if the engine ID is 12345, the ID is treated as 12.34.05 internally. Hence, the engine ID is displayed as 123405 in the <code>show running configuration</code> command output.</p><p>Changing the value of the SNMP engine ID has significant effects. A user's password (entered on the command line) is converted to a message digest's algorithm (MD5) or Secure Hash Algorithm (SHA) security digest. This digest is based on both the password and the local engine ID. The command line password is then destroyed, as required by RFC 2274. Because of this deletion, if the local value of the engineID changes, the security digests of SNMPv3 users will become invalid, and the users will have to be reconfigured.</p><p>Similar restrictions require the reconfiguration of community strings when the engine ID changes. A remote engine ID is required when an SNMPv3 inform is configured. The remote engine ID is used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host.</p></div></div><div><div>Examples</div><div><p>The following example specifies the local SNMP engine ID:</p><pre>Router#(config)# snmp-server engineID local</pre></div></div></div> <div>Cisco IOS 15.4</div> <div>Effective date of registration: 11/26/2014</div>	Release	Modification	12.0(3)T	This command was introduced.	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.	<div><div>snmp-server engineID local</div><div>The <code>snmp-server engineID local</code> command configures the name for the local Simple Network Management Protocol (SNMP) engine. The default SNMP engineID is generated by the switch and is used when an engineID is not configured with this command. The <code>show snmp engineID</code> command displays the default or configured engine ID.</div><div>SNMPv3 authenticates users through security digests (MD5 or SHA) that are based on user passwords and the local engine ID. Passwords entered on the CLI are similarly converted, then compared to the user's security digest to authenticate the user.</div><div><div>Important</div><div>Changing the local engineID value invalidates SNMPv3 security digests, requiring the reconfiguration of all user passwords.</div></div><div>The no snmp-server engineID and default snmp-server engineID commands restore the default engineID by removing the snmp-server engineID command from the configuration.</div><div><div>Platform</div><div>all</div><div>Command Mode</div><div>Global Configuration</div></div><div><div>Command Syntax</div><div><div>snmp-server engineID local engine_hex</div><div>no snmp-server engineID local</div><div>default snmp-server engineID</div></div></div><div><div>Parameters</div><div><ul style="list-style-type: none">engine_hex the switch's name for the local SNMP engine (hex string).<p>The string must consist of at least ten characters with a maximum of 64 characters.</p></div></div><div><div>Example</div><div><ul style="list-style-type: none">This command configures DC945798CAB4 as the name of the local SNMP engine.<pre>switch(config)#snmp-server engineID local DC945798CAB4 switch(config)#</pre></div></div><div><div>snmp-server engineID remote</div><div>The snmp-server engineID remote command configures the name of a Simple Network Management Protocol (SNMP) engine located on a remote device. The switch generates a default engineID; use the <code>show snmp engineID</code> command to view the configured or default engineID.</div><div>A remote engine ID is required when configuring an SNMPv3 inform to compute the security digest for authenticating and encrypting packets sent to users on the remote host. SNMPv3 authenticates users through security digests (MD5 or SHA) that are based on user passwords and the engine ID. Passwords entered on the CLI are similarly converted, then compared to the user's security digest to authenticate the user.</div></div><div>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1991-92.</div><div>See also Arista User Manual v. 4.12.3 (7/17/13), at 1681-82; Arista User Manual, v. 4.11.1 (1/11/13), at 1366-67; Arista User Manual v. 4.10.3 (10/22/12), at 1133-34; Arista User Manual v. 4.9.3.2 (5/3/12), at 889-890; Arista User Manual v. 4.8.2 (11/18/11), at 697-98; Arista User</div></div>
Release	Modification									
12.0(3)T	This command was introduced.									
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.									
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.									

Copyright Registration Information	Cisco	Arista				
		Manual v. 4.7.3 (7/18/11), at 553-54.				
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<table><tr><th>Command</th><th>Description</th></tr><tr><td>show snmp engineID</td><td>Displays the identification of the local SNMP engine and all remote engines that have been configured on the router.</td></tr></table>	Command	Description	show snmp engineID	Displays the identification of the local SNMP engine and all remote engines that have been configured on the router.	show snmp engineID The show snmp engineID command displays the identification of the local Simple Network Management Protocol (SNMP) engine and of all remote engines that are configured on the switch.
	Command	Description				
show snmp engineID	Displays the identification of the local SNMP engine and all remote engines that have been configured on the router.					
	Cisco IOS SNMP Support Command Reference (2013), at 340/	Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1978. See also Arista User Manual v. 4.12.3 (7/17/13), at 1668; Arista User Manual, v. 4.11.1 (1/11/13), at 1355; Arista User Manual v. 4.10.3 (10/22/12), at 1122; Arista User Manual v. 4.9.3.2 (5/3/12), at 878; Arista User Manual v. 4.8.2 (11/18/11), at 686; Arista User Manual v. 4.7.3 (7/18/11), at 542.				

Copyright Registration Information	Cisco	Arista																				
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<div>snmp-server group</div> <div>To configure a new Simple Network Management Protocol (SNMP) group, use the <code>snmp-server group</code> command in global configuration mode. To remove a specified SNMP group, use the <code>no</code> form of this command.</div> <div>snmp-server group group-name {v1 v2c v3} {auth noauth priv} {context context-name} [read read-view] [write write-view] [notify notify-view] [access {ipv6 named-access-list} [acl-number] acl-name]] no snmp-server group group-name {v1 v2c v3} {auth noauth priv} {context context-name}</div> <div>Syntax Description</div> <table><tr><th>group-name</th><th>Name of the group.</th></tr><tr><td>v1</td><td>Specifies that the group is using the SNMPv1 security model. SNMPv1 is the least secure of the possible SNMP security models.</td></tr><tr><td>v2c</td><td>Specifies that the group is using the SNMPv2c security model. The SNMPv2c security model allows informs to be transmitted and supports 64-character strings.</td></tr><tr><td>v3</td><td>Specifies that the group is using the SNMPv3 security model. SNMPv3 is the most secure of the supported security models. It allows you to explicitly configure authentication characteristics.</td></tr><tr><td>auth</td><td>Specifies authentication of a packet without encrypting it.</td></tr><tr><td>noauth</td><td>Specifies no authentication of a packet.</td></tr><tr><td>priv</td><td>Specifies authentication of a packet with encryption.</td></tr><tr><td>context</td><td>(Optional) Specifies the SNMP context to associate with this SNMP group and its views.</td></tr><tr><td>context-name</td><td>(Optional) Context name.</td></tr><tr><td>read</td><td>(Optional) Specifies a read view for the SNMP group. This view enables you to view only the contents of the agent.</td></tr></table>	group-name	Name of the group.	v1	Specifies that the group is using the SNMPv1 security model. SNMPv1 is the least secure of the possible SNMP security models.	v2c	Specifies that the group is using the SNMPv2c security model. The SNMPv2c security model allows informs to be transmitted and supports 64-character strings.	v3	Specifies that the group is using the SNMPv3 security model. SNMPv3 is the most secure of the supported security models. It allows you to explicitly configure authentication characteristics.	auth	Specifies authentication of a packet without encrypting it.	noauth	Specifies no authentication of a packet.	priv	Specifies authentication of a packet with encryption.	context	(Optional) Specifies the SNMP context to associate with this SNMP group and its views.	context-name	(Optional) Context name.	read	(Optional) Specifies a read view for the SNMP group. This view enables you to view only the contents of the agent.	<div>snmp-server group</div> <div>The <code>snmp-server group</code> command configures a new Simple Network Management Protocol (SNMP) group or modifies an existing group. An SNMP group is a data structure that user statements reference to map SNMP users to SNMP contexts and views, providing a common access policy to the specified users.</div> <div>An SNMP context is a collection of management information items accessible by an SNMP entity. Each item of may exist in multiple contexts. Each SNMP entity can access multiple contexts. A context is identified by the EngineID of the hosting device and a context name.</div> <div>The <code>no snmp-server group</code> and <code>default snmp-server group</code> commands delete the specified group by removing the corresponding <code>snmp-server group</code> command from the configuration.</div> <div>Platform all Command Mode Global Configuration</div> <div>Command Syntax</div> <div>snmp-server group group_name VERSION [CNTX] [READ] [WRITE] [NOTIFY] no snmp-server group group_name VERSION default snmp-server group group_name VERSION</div> <div>Parameters</div> <ul style="list-style-type: none">group_name the name of the group.VERSION the security model used by the group.<ul style="list-style-type: none">v1 SNMPv1. Uses a community string match for authentication.v2c SNMPv2c. Uses a community string match for authentication.v3 no auth SNMPv3. Uses a username match for authentication.v3 auth SNMPv3. HMAC-MD5 or HMAC-SHA authentication.v3 priv SNMPv3. HMAC-MD5 or HMAC-SHA authentication. AES or DES encryption.CNTX associates the SNMP group to an SNMP context.<ul style="list-style-type: none"><no parameter> command does not associate group with an SNMP context.context context_name associates group with context specified by context_name.READ specifies read view for SNMP group.<ul style="list-style-type: none"><no parameter> command does not specify read view.read read_name read view specified by read_name (string – maximum 64 characters).WRITE specifies write view for SNMP group.<ul style="list-style-type: none"><no parameter> command does not specify write view.write write_name write view specified by write_name (string – maximum 64 characters).NOTIFY specifies notify view for SNMP group.<ul style="list-style-type: none"><no parameter> command does not specify notify view.notify notify_name notify view specified by notify_name (string – maximum 64 characters).
	group-name	Name of the group.																				
v1	Specifies that the group is using the SNMPv1 security model. SNMPv1 is the least secure of the possible SNMP security models.																					
v2c	Specifies that the group is using the SNMPv2c security model. The SNMPv2c security model allows informs to be transmitted and supports 64-character strings.																					
v3	Specifies that the group is using the SNMPv3 security model. SNMPv3 is the most secure of the supported security models. It allows you to explicitly configure authentication characteristics.																					
auth	Specifies authentication of a packet without encrypting it.																					
noauth	Specifies no authentication of a packet.																					
priv	Specifies authentication of a packet with encryption.																					
context	(Optional) Specifies the SNMP context to associate with this SNMP group and its views.																					
context-name	(Optional) Context name.																					
read	(Optional) Specifies a read view for the SNMP group. This view enables you to view only the contents of the agent.																					

Copyright Registration Information	Cisco	Arista	
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<i>read-view</i>	(Optional) String of a maximum of 64 characters that is the name of the view. The default is that the read-view is assumed to be every object belonging to the Internet object identifier (OID) space (1.3.6.1), unless the read option is used to override this state.	Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1994. <i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1684; Arista User Manual, v. 4.11.1 (1/11/13), at 1369; Arista User Manual v. 4.10.3 (10/22/12), at 1136; Arista User Manual v. 4.9.3.2 (5/3/12), at 892; Arista User Manual v. 4.8.2 (11/18/11), at 699; Arista User Manual v. 4.7.3 (7/18/11), at 555.
	write	(Optional) Specifies a write view for the SNMP group. This view enables you to enter data and configure the contents of the agent.	
	<i>write-view</i>	(Optional) String of a maximum of 64 characters that is the name of the view. The default is that nothing is defined for the write view (that is, the null OID). You must configure write access.	
	notify	(Optional) Specifies a notify view for the SNMP group. This view enables you to specify a notify, inform, or trap.	
	<i>notify-view</i>	(Optional) String of a maximum of 64 characters that is the name of the view. By default, nothing is defined for the notify view (that is, the null OID) until the snmp-server host command is configured. If a view is specified in the snmp-server group command, any notifications in that view that are generated will be sent to all users associated with the group (provided a SNMP server host configuration exists for the user). Cisco recommends that you let the software autogenerate the notify view. See the "Configuring Notify Views" section in this document.	
	access	(Optional) Specifies a standard access control list (ACL) to associate with the group.	
	ipv6	(Optional) Specifies an IPv6 named access list. If both IPv6 and IPv4 access lists are indicated, the IPv6 named access list must appear first in the list.	
	<i>named-access-list</i>	(Optional) Name of the IPv6 access list.	
	<i>acl-number</i>	(Optional) The <i>acl-number</i> argument is an integer from 1 to 99 that identifies a previously configured standard access list.	
	Cisco IOS SNMP Support Command Reference (2013), at 343-44.		

Copyright Registration Information	Cisco	Arista							
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<div><div>■</div><div>snmp-server host</div></div> <table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>Cisco IOS XE Release 2.1</td><td>This command was integrated into Cisco IOS XE Release 2.1.</td></tr><tr><td>15.2(1)S</td><td>This command was modified. The p2mp-traffic-eng notification-type keyword was added.</td></tr></tbody></table> <div>Usage Guidelines</div> <p>If you enter this command with no optional keywords, the default is to send all notification-type traps to the host. No informs will be sent to the host.</p> <p>The no snmp-server host command with no keywords disables traps, but not informs, to the host. To disable informs, use the no snmp-server host informs command.</p> <div><div></div><div>Note</div></div> <p>If a community string is not defined using the snmp-server community command prior to using this command, the default form of the snmp-server community command will automatically be inserted into the configuration. The password (community string) used for this automatic configuration of the snmp-server community command will be the same as that specified in the snmp-server host command. This automatic command insertion and use of passwords is the default behavior for Cisco IOS Release 12.0(3) and later releases. However, in Cisco IOS Release 12.2(33)SRE and later releases, you must manually configure the snmp-server community command. That is, the snmp-server community command will not be seen in the configuration.</p>	Release	Modification	Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.	15.2(1)S	This command was modified. The p2mp-traffic-eng notification-type keyword was added.	<div><div></div><div>snmp-server host</div></div> <p>The snmp-server host command specifies the recipient of Simple Network Management Protocol (SNMP) notifications. Recipients are denoted by host location and community string. The command also specifies the type of SNMP notifications that are sent: a <i>trap</i> is an unsolicited notification; an <i>inform</i> is a trap that includes a request for a confirmation that the message is received.</p> <p>The configuration can contain multiple statements to the same host location with different community strings. For instance, a configuration can simultaneously contain all of the following:</p> <ul style="list-style-type: none">• snmp-server host host-1 version 2c comm-1• snmp-server host host-1 informs version 2c comm-2• snmp-server host host-1 version 2c comm-3 udp-port 666• snmp-server host host-1 version 3 auth comm-3 <p>The no snmp-server host and default snmp-server host commands remove the specified host by deleting the corresponding snmp-server host statement from the configuration. When removing a statement, the host (address and port) and community string must be specified.</p> <div><div>Platform</div><div>all</div></div> <div><div>Command Mode</div><div>Global Configuration</div></div> <div>Command Syntax</div> <pre>snmp-server host host_id [VRF INST] [MESSAGE] [VERSION] comm_str [PORT] no snmp-server host host_id [VRF INST] [MESSAGE] [VERSION] comm_str [PORT] default snmp-server host host_id [VRF INST] [MESSAGE] [VERSION] comm_str [PORT]</pre> <div>Parameters</div> <ul style="list-style-type: none">• host_id hostname or IP address of the targeted recipient.• VRF_INST specifies the VRF instance being modified.<ul style="list-style-type: none">— <no parameter> changes are made to the default VRF.— vrf vrf_name changes are made to the specified user-defined VRF.• MESSAGE message type that is sent to the host.<ul style="list-style-type: none">— <no parameter> sends SNMP traps to host (default).— informs sends SNMP informs to host.— traps sends SNMP traps to host.• VERSION SNMP version. Options include:<ul style="list-style-type: none">— <no parameter> SNMPv2c (default).— version 1 SNMPv1; option not available with informs.— version 2c SNMPv2c.— version 3 noauth SNMPv3; enables user-name match authentication.— version 3 auth SNMPv3; enables MD5 and SHA packet authentication.— version 3 priv SNMPv3. HMAC-MD5 or HMAC-SHA authentication. AES or DES encryption.• comm_str community string (used as password) sent with the notification operation. <p>Although this string can be set with the snmp-server host command, the preferred method is defining it with the snmp-server community command prior to using this command.</p>	Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1995. See also Arista User Manual v. 4.12.3 (7/17/13), at 1685; Arista User
	Release	Modification							
	Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.							
15.2(1)S	This command was modified. The p2mp-traffic-eng notification-type keyword was added.								

Copyright Registration Information	Cisco	Arista
		Manual, v. 4.11.1 (1/11/13), at 1370; Arista User Manual v. 4.10.3 (10/22/12), at 1137; Arista User Manual v. 4.9.3.2 (5/3/12), at 893; Arista User Manual v. 4.8.2 (11/18/11), at 700; Arista User Manual v. 4.7.3 (7/18/11), at 556.
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<p>SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response protocol data unit (PDU). If the sender never receives the response, the inform request can be sent again. Thus, informs are more likely to reach their intended destination than traps.</p> <p>Compared to traps, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Also, traps are sent only once; an inform may be tried several times. The retries increase traffic and contribute to a higher overhead on the network.</p> <p>Cisco IOS SNMP Support Command Reference (2013), at 354.</p>	<p>SNMP notifications are messages, sent by the agent, to inform managers of an event or a network condition. A <i>trap</i> is an unsolicited notification. An <i>inform</i> (or inform request) is a trap that includes a request for a confirmation that the message is received. Events that a notification can indicate include improper user authentication, restart, and connection losses.</p> <p>Traps are less reliable than informs because the receiver does not send any acknowledgment. However, traps are often preferred because informs consume more switch and network resources. A trap is sent only once and is discarded as soon as it is sent. An inform request remains in memory until a response is received or the request times out. An inform may be retried several times, increasing traffic and contributing to higher network overhead.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1963.</p> <p><i>See also</i> Arista User Manual v. 4.13.6F (4/14/2014), at 1891; Arista User Manual v. 4.12.3 (7/17/13), at 1653; Arista User Manual, v. 4.11.1 (1/11/13), at 1341; Arista User Manual v. 4.10.3 (10/22/12), at 1107; Arista User Manual v. 4.9.3.2 (5/3/12), at 863; Arista User Manual v. 4.8.2 at 675; Arista User Manual v. 4.7.3 (7/18/11), at 531.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<p>snmp-server source-interface</p> <p>To specify the interface from which a Simple Network Management Protocol (SNMP) trap originates the informs or traps, use the snmp-server source-interface command in global configuration mode. To remove the source designation, use the no form of this command.</p> <p>snmp-server source-interface {traps informs} <i>interface</i> no snmp-server source-interface {traps informs} [<i>interface</i>]</p> <p>Cisco IOS SNMP Support Command Reference (2013), at 376.</p>	<p>snmp-server source-interface</p> <p>The snmp-server source-interface command specifies the interface from which a Simple Network Management Protocol (SNMP) trap originates the informs or traps.</p> <p>The no snmp-server source-interface and default snmp-server source-interface commands remove the inform or trap source assignment by removing the snmp-server source-interface command from running-config.</p> <p>Platform all Command Mode Global Configuration</p> <p>Command Syntax</p> <p>snmp-server source-interface <i>INTERFACE</i> no snmp-server source-interface default snmp-server source-interface</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1967.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1688; Arista User Manual, v. 4.11.1 (1/11/13), at 1373; Arista User Manual v. 4.10.3 (10/22/12), at 1140; Arista User Manual v. 4.9.3.2 (5/3/12), at 895; Arista User Manual v. 4.8.2 (11/18/11), at 702; Arista User Manual v. 4.7.3 (7/18/11), at 558.</p>

Copyright Registration Information	Cisco	Arista																						
Copyright Registration Information	<div>snmp-server user</div> <div>To configure a new user to a Simple Network Management Protocol (SNMP) group, use the snmp-server user command in global configuration mode. To remove a user from an SNMP group, use the no form of this command.</div> <div>snmp-server user username group-name [remote host [udp-port port] [vrf vrf-name]] {v1 v2c v3} [encrypted] [auth {md5 sha} auth-password] [access {ipv6 naci} [priv {des 3des aes (128 192 256)} privpassword] {acl-number acl-name}]]</div> <div>no snmp-server user username group-name [remote host [udp-port port] [vrf vrf-name]] {v1 v2c v3} [encrypted] [auth {md5 sha} auth-password] [access {ipv6 naci} [priv {des 3des aes (128 192 256)} privpassword] {acl-number acl-name}]]</div> <div>Syntax Description</div> <table><tr><td>username</td><td>Name of the user on the host that connects to the agent.</td></tr><tr><td>group-name</td><td>Name of the group to which the user belongs.</td></tr><tr><td>remote</td><td>(Optional) Specifies a remote SNMP entity to which the user belongs, and the hostname or IPv6 address or IPv4 IP address of that entity. If both an IPv6 address and IPv4 IP address are being specified, the IPv6 host must be listed first.</td></tr><tr><td>host</td><td>(Optional) Name or IP address of the remote SNMP host.</td></tr><tr><td>udp-port</td><td>(Optional) Specifies the User Datagram Protocol (UDP) port number of the remote host.</td></tr><tr><td>port</td><td>(Optional) Integer value that identifies the UDP port. The default is 162.</td></tr><tr><td>vrf</td><td>(Optional) Specifies an instance of a routing table.</td></tr><tr><td>vrf-name</td><td>(Optional) Name of the Virtual Private Network (VPN) routing and forwarding (VRF) table to use for storing data.</td></tr><tr><td>v1</td><td>Specifies that SNMPv1 should be used.</td></tr><tr><td>v2c</td><td>Specifies that SNMPv2c should be used.</td></tr><tr><td>v3</td><td>Specifies that the SNMPv3 security model should be used. Allows the use of the encrypted keyword or auth keyword or both.</td></tr></table>	username	Name of the user on the host that connects to the agent.	group-name	Name of the group to which the user belongs.	remote	(Optional) Specifies a remote SNMP entity to which the user belongs, and the hostname or IPv6 address or IPv4 IP address of that entity. If both an IPv6 address and IPv4 IP address are being specified, the IPv6 host must be listed first.	host	(Optional) Name or IP address of the remote SNMP host.	udp-port	(Optional) Specifies the User Datagram Protocol (UDP) port number of the remote host.	port	(Optional) Integer value that identifies the UDP port. The default is 162.	vrf	(Optional) Specifies an instance of a routing table.	vrf-name	(Optional) Name of the Virtual Private Network (VPN) routing and forwarding (VRF) table to use for storing data.	v1	Specifies that SNMPv1 should be used.	v2c	Specifies that SNMPv2c should be used.	v3	Specifies that the SNMPv3 security model should be used. Allows the use of the encrypted keyword or auth keyword or both.	<div>snmp-server user</div> <div>The snmp-server user command adds a user to a Simple Network Management Protocol (SNMP) group or modifies an existing user's parameters.</div> <div>To configure a remote user, specify the IP address or port number of the device where the user's remote SNMP agent resides. A remote agent's engine ID must be configured before remote users for that agent are configured. A user's authentication and privacy digests are derived from the engine ID and the user's password. The configuration command fails if the remote engine ID is not configured first.</div> <div>The no snmp-server user and default snmp-server user commands remove the user from an SNMP group by deleting the user command from running-config.</div> <div>Platform all Command Mode Global Configuration</div> <div>Command Syntax</div> <div>snmp-server user user name group name [AGENT] VERSION [ENGINE] [SECURITY] no snmp-server user user name group name [AGENT] VERSION default snmp-server user user_name group_name [AGENT] VERSION</div> <div>Parameters</div> <div><ul style="list-style-type: none">user name name of the user on the host that connects to the agent.group name name of the group to which the user is associated.AGENT location of the host connecting to the SNMP agent. Configuration options include:<ul style="list-style-type: none"><no parameter> local SNMP agent.remote:addr [udp-port p_num] remote SNMP agent location (IP address, udp port). addr denotes the IP address; p_num denotes the udp port socket. (default port is 162).VERSION SNMP version; options include:<ul style="list-style-type: none">v1 SNMPv1.v2c SNMPv2c.v3 SNMPv3; enables user-name match authentication.ENGINE engine ID used to localize passwords. Available only if VERSION is v3.<ul style="list-style-type: none"><no parameter> Passwords localized by SNMP copy specified by agent.localized engineID octet string of engineID.SECURITY Specifies authentication and encryption levels. Available only if VERSION is v3. Encryption is available only when authentication is configured.<ul style="list-style-type: none"><no parameter> no authentication or encryption.auth a_meth a_pass [priv e_meth e_pass] authentication and encryption parameters. a_meth authentication method: options are md5 (HMAC-MD5-96) and sha (HMAC-SHA-96). a_pass authentication string for users receiving packets. e_meth encryption method: tions are aes (AES-128) and des (CBC-DES). e_pass encryption string for the users sending packets.</div>
	username	Name of the user on the host that connects to the agent.																						
group-name	Name of the group to which the user belongs.																							
remote	(Optional) Specifies a remote SNMP entity to which the user belongs, and the hostname or IPv6 address or IPv4 IP address of that entity. If both an IPv6 address and IPv4 IP address are being specified, the IPv6 host must be listed first.																							
host	(Optional) Name or IP address of the remote SNMP host.																							
udp-port	(Optional) Specifies the User Datagram Protocol (UDP) port number of the remote host.																							
port	(Optional) Integer value that identifies the UDP port. The default is 162.																							
vrf	(Optional) Specifies an instance of a routing table.																							
vrf-name	(Optional) Name of the Virtual Private Network (VPN) routing and forwarding (VRF) table to use for storing data.																							
v1	Specifies that SNMPv1 should be used.																							
v2c	Specifies that SNMPv2c should be used.																							
v3	Specifies that the SNMPv3 security model should be used. Allows the use of the encrypted keyword or auth keyword or both.																							
Cisco IOS 15.4	Cisco IOS SNMP Support Command Reference (2013), at 394.	Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1999.																						
Effective date of registration: 11/26/2014		See also Arista User Manual v. 4.12.3 (7/17/13), at 1689; Arista User Manual, v. 4.11.1 (1/11/13), at 1374; Arista User Manual v. 4.10.3																						

Copyright Registration Information	Cisco	Arista
		(10/22/12), at 1141; Arista User Manual v. 4.9.3.2 (5/3/12), at 896; Arista User Manual v. 4.8.2 (11/18/11), at 703; Arista User Manual v. 4.7.3 (7/18/11), at 559.
<p>Cisco IOS 15.4</p> <p>Effective date of registration: 11/26/2014</p>	<p>Usage Guidelines To configure a remote user, specify the IP address or port number for the remote SNMP agent of the device where the user resides. Also, before you configure remote users for a particular agent, configure the SNMP engine ID, using the <code>snmp-server engineID</code> command with the remote keyword. The remote agent's SNMP engine ID is needed when computing the authentication and privacy digests from the password. If the remote engine ID is not configured first, the configuration command will fail.</p> <p>For the <code>privpassword</code> and <code>auth-password</code> arguments, the minimum length is one character; the recommended length is at least eight characters, and should include both letters and numbers.</p> <p>Cisco IOS SNMP Support Command Reference (2013), at 396.</p>	<p>To configure a remote user, specify the IP address or port number of the device where the user's remote SNMP agent resides. A remote agent's engine ID must be configured before remote users for that agent are configured. A user's authentication and privacy digests are derived from the engine ID and the user's password. The configuration command fails if the remote engine ID is not configured first.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) 10/2/2014), at 1999.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1689; Arista User Manual, v. 4.11.1 (1/11/13), at 1374; Arista User Manual v. 4.10.3 (10/22/12), at 1141; Arista User Manual v. 4.9.3.2 (5/3/12), at 896; Arista User Manual v. 4.8.2 (11/18/11), at 703; Arista User Manual v. 4.7.3 (7/18/11), at 559.</p>

Copyright Registration Information	Cisco	Arista								
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<div>timers basic (ISO CLNS)</div> <p>To configure ISO IGRP timers, use the timers basic command in router configuration mode. To restore the default values, use the no form of this command.</p> <div>timers basic update-interval holddown-interval invalid-interval</div> <div>no timers basic update-interval holddown-interval invalid-interval</div> <table><tr><td>Syntax</td><td>Description</td></tr><tr><td>update-interval</td><td>Time, in seconds, between the sending of routing updates.</td></tr><tr><td>holddown-interval</td><td>Time, in seconds, a system or area router is kept in holddown state, during which routing information regarding better paths is suppressed. (A router enters into a holddown state when an update packet is received that indicates the route is unreachable. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets.) When the holddown interval expires, routes advertised by other sources are accepted and the route is no longer inaccessible.</td></tr><tr><td>invalid-interval</td><td>Time, in seconds, that a route remains in the routing table after it has been determined that it is not reachable. After that length of time, the route is removed from the routing table.</td></tr></table> <p>Cisco IOS Interface and Hardware Component Command Reference (2011), at ISO-178.</p>	Syntax	Description	update-interval	Time, in seconds, between the sending of routing updates.	holddown-interval	Time, in seconds, a system or area router is kept in holddown state, during which routing information regarding better paths is suppressed. (A router enters into a holddown state when an update packet is received that indicates the route is unreachable. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets.) When the holddown interval expires, routes advertised by other sources are accepted and the route is no longer inaccessible.	invalid-interval	Time, in seconds, that a route remains in the routing table after it has been determined that it is not reachable. After that length of time, the route is removed from the routing table.	<div>timers basic (RIP)</div> <p>The timers basic command configures the update interval, the expiration time, and the deletion time for routes received and sent through RIP. The command requires value declaration of all values.</p> <ul style="list-style-type: none">The update time is the interval between unsolicited route responses. The default is 30 seconds.The expiration time is initialized when a route is established and any time an update is received for the route. If the specified period elapses from the last time the route update was received, then the route is marked as inaccessible and advertised as unreachable. However, the route forwards packets until the deletion time expires. The default value is 180 seconds.The deletion time is initialized when the expiration time has elapsed. On initialization of the deletion time, the route is no longer valid; however, it is retained in the routing table for a short time so that neighbors can be notified that the route has been dropped. Upon expiration of the deletion time, the route is removed from the routing table. The default is 120 seconds. <p>The no timers basic and default timers basic commands return the timer values to their default values by removing the timers-basic command from <i>running-config</i>.</p> <div>Platformall</div> <div>Command ModeRouter-RIP Configuration</div> <p>Command Syntax</p> <div>timers basic update_time expire_time deletion_time</div> <div>no timers basic</div> <div>default timers basic</div> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1671.</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 1621; Arista User Manual v. 4.12.3 (7/17/13), at 1433; Arista User Manual, v. 4.11.1 (1/11/13), at 1179; Arista User Manual v. 4.10.3 (10/22/12), at 989; Arista User Manual v. 4.9.3.2 (5/3/12), at 748; ; Arista User Manual v. 4.8.2 (11/18/11), at 570.</p>
	Syntax	Description								
update-interval	Time, in seconds, between the sending of routing updates.									
holddown-interval	Time, in seconds, a system or area router is kept in holddown state, during which routing information regarding better paths is suppressed. (A router enters into a holddown state when an update packet is received that indicates the route is unreachable. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets.) When the holddown interval expires, routes advertised by other sources are accepted and the route is no longer inaccessible.									
invalid-interval	Time, in seconds, that a route remains in the routing table after it has been determined that it is not reachable. After that length of time, the route is removed from the routing table.									


Copyright Registration Information	Cisco	Arista																
Cisco IOS 15.4 Effective date of registration: 11/26/2014	<table><thead><tr><th>Field</th><th>Description</th></tr></thead><tbody><tr><td>Version 34</td><td>Indicates version number of the Level 1 routing table. All Level 1 routes with a version number that does not match this number are flushed from the routing table. The router's version number increments when the configuration changes from Level 1 or Level 1-2 to Level 2 only.</td></tr><tr><td>System Id</td><td>Identification value of the system listed in Level 1 forwarding table.</td></tr><tr><td>Next-Hop</td><td>System ID of best-cost next-hop to listed address.</td></tr><tr><td>SNPA</td><td>SNPA of next-hop system.</td></tr><tr><td>Interface</td><td>Interface through which next-hop system is known.</td></tr><tr><td>Metric</td><td>IS-IS metric for the route.</td></tr><tr><td>State</td><td>Up (active) or Down (nonoperational).</td></tr></tbody></table> <p>Cisco IOS Interface and Hardware Component Command Reference (2011), at ISO-137.</p>	Field	Description	Version 34	Indicates version number of the Level 1 routing table. All Level 1 routes with a version number that does not match this number are flushed from the routing table. The router's version number increments when the configuration changes from Level 1 or Level 1-2 to Level 2 only.	System Id	Identification value of the system listed in Level 1 forwarding table.	Next-Hop	System ID of best-cost next-hop to listed address.	SNPA	SNPA of next-hop system.	Interface	Interface through which next-hop system is known.	Metric	IS-IS metric for the route.	State	Up (active) or Down (nonoperational).	<p>Display Values</p> <ul style="list-style-type: none">• Inst. ID IS-IS Instance name.• System ID Identification value of the system listed in the Level 2 forwarding table• Type Level 2 information.• Interface Interface through which the neighbor is reachable.• SNPA Subnetwork point of attachment (MAC address of the next hop).• State State of the adjacency: Up, Down, or INIT• Hold time Remaining hold time of the adjacency.• Area Address The address of the area. <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1702.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1459.</p>
Field	Description																	
Version 34	Indicates version number of the Level 1 routing table. All Level 1 routes with a version number that does not match this number are flushed from the routing table. The router's version number increments when the configuration changes from Level 1 or Level 1-2 to Level 2 only.																	
System Id	Identification value of the system listed in Level 1 forwarding table.																	
Next-Hop	System ID of best-cost next-hop to listed address.																	
SNPA	SNPA of next-hop system.																	
Interface	Interface through which next-hop system is known.																	
Metric	IS-IS metric for the route.																	
State	Up (active) or Down (nonoperational).																	
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<p>Building the Address Table and Address Table Changes</p> <p>The device dynamically builds the address table by using the MAC source address of the frames received. When the device receives a frame for a MAC destination address not listed in its address table, it floods the frame to all LAN ports of the same VLAN except the port that received the frame. When the destination station replies, the device adds its relevant MAC source address and port ID to the address table. The device then forwards subsequent frames to a single LAN port without flooding all LAN ports.</p> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide (2011), at 10.</p>	<p>14.3 MAC Address Table</p> <p>The switch maintains an MAC address table for switching frames efficiently between ports. The MAC address table contains static and dynamic MAC addresses.</p> <ul style="list-style-type: none">• Static MAC addresses are entered into the table through a CLI command.• Dynamic MAC addresses are entered into the table when the switch receives a frame whose source address is not listed in the MAC address table. The switch builds the table dynamically by referencing the source address of frames it receives. <p>When the switch receives a frame, it associates the MAC address of the transmitting interface with the recipient VLAN. When a VLAN receives a frame for a MAC destination address not listed in the address table, the switch bridges the frame to all of the VLAN's ports except the recipient port. When the destination interface replies, the switch adds its MAC address to the MAC address table. The switch forwards subsequent frames with the destination address to the specified port.</p> <p>A multicast address can be associated with multiple ports.</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 624.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 494; Arista User Manual, v. 4.11.1 (1/11/13), at 396-97; Arista User Manual v. 4.10.3 (10/22/12), at 328; Arista User Manual v. 4.9.3.2 (5/3/12), at 306.</p>																


Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>• Community VLAN—A community VLAN is a secondary VLAN that carries upstream traffic from the community ports to the promiscuous port gateways and to other host ports in the same community. You can configure multiple community VLANs in a private VLAN domain. The ports within one community can communicate, but these ports cannot communicate with ports in any other community or isolated VLAN in the private VLAN.</p> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide (2011), at 54.</p>	<p>— Community Community VLAN ports carry traffic from host ports to the primary VLAN ports and to other host ports in the same community VLAN.</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 763.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 611; Arista User Manual, v. 4.11.1 (1/11/13), at 467; Arista User Manual v. 4.10.3 (10/22/12), at 387; Arista User Manual v. 4.9.3.2 (5/3/12), at 307.</p>
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>• Protocol migration—For backward compatibility with 802.1D devices, 802.1w selectively sends 802.1D configuration BPDUs and TCN BPDUs on a per-port basis.</p> <p>When a port is initialized, the migrate-delay timer is started (specifies the minimum time during which 802.1w BPDUs are sent), and 802.1w BPDUs are sent. While this timer is active, the device processes all BPDUs received on that port and ignores the protocol type.</p> <p>If the device receives an 802.1D BPDU after the port migration-delay timer has expired, it assumes that it is connected to an 802.1D device and starts using only 802.1D BPDUs. However, if the 802.1w device is using 802.1D BPDUs on a port and receives an 802.1w BPDU after the timer has expired, it restarts the timer and starts using 802.1w BPDUs on that port.</p> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide (2011), at 100</p>	<p>The clear spanning-tree detected-protocols command forces MST ports to renegotiate with their neighbors.</p> <p>RSTP provides backward compatibility with 802.1D bridges as follows:</p> <ul style="list-style-type: none"> • RSTP selectively sends 802.1D-configured BPDUs and Topology Change Notification (TCN) BPDUs on a per-port basis. • When a port initializes, the migration delay timer starts and RSTP BPDUs are transmitted. While the migration delay timer is active, the bridge processes all BPDUs received on that port. • If the bridge receives an 802.1D BPDU after a port's migration delay timer expires, the bridge assumes it is connected to an 802.1D bridge and starts using only 802.1D BPDUs. • When RSTP uses 802.1D BPDUs on a port and receives an RSTP BPDU after the migration delay expires, RSTP restarts the migration delay timer and resumes using RSTP BPDUs on that port. <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 953.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 831; Arista User Manual, v. 4.11.1 (1/11/13), at 649; Arista User Manual v. 4.10.3 (10/22/12), at 563; Arista User Manual v. 4.9.3.2 (5/3/12), at 483; Arista User Manual v. 4.8.2 (11/18/11), at 357; Arista User Manual v. 4.7.3 (7/18/11), at 231.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>Loop Guard</p> <p>Loop Guard helps prevent bridging loops that could occur because of a unidirectional link failure on a point-to-point link.</p> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide (2011), at 176.</p>	<ul style="list-style-type: none"> • Loop Guard: Prevents loops resulting from a unidirectional link failure on a point-to-point link. <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 963.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 842; Arista User Manual, v. 4.11.1 (1/11/13), at 660; Arista User Manual v. 4.10.3 (10/22/12), at 574; Arista User Manual v. 4.9.3.2 (5/3/12), at 494; Arista User Manual v. 4.8.2 (11/18/11), at 368; Arista User Manual v. 4.7.3 (7/18/11), at 242.</p>
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>Rapid PVST+ achieves rapid transition to the forwarding state only on edge ports and point-to-point links.</p> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide (2011), at 90.</p>	<p>RSTP only achieves rapid transition to forwarding state on edge ports and point-to-point links.</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 964.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 843; Arista User Manual, v. 4.11.1 (1/11/13), at 661; Arista User Manual v. 4.10.3 (10/22/12), at 575; Arista User Manual v. 4.9.3.2 (5/3/12), at 494; Arista User Manual v. 4.8.2 (11/18/11), at 368; Arista User Manual v. 4.7.3 (7/18/11), at 242.</p>
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>Enabling Loop Guard on a root device has no effect but provides protection when a root device becomes a nonroot device.</p> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide (2011), at 176.</p>	<p>Enabling loop guard on a root switch has no effect until the switch becomes a nonroot switch.</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 966.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 844; Arista User Manual, v. 4.11.1 (1/11/13), at 662; Arista User Manual v. 4.10.3 (10/22/12), at 576; Arista User Manual v. 4.9.3.2 (5/3/12), at 496; Arista User Manual v. 4.8.2 (11/18/11), at 370; Arista User Manual v. 4.7.3 (7/18/11), at 244.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<ul style="list-style-type: none"> Enabling Loop Guard globally works only on point-to-point links. Enabling Loop Guard per interface works on both shared and point-to-point links. Root Guard forces a port to always be a designated port; it does not allow a port to become a root port. Loop Guard is effective only if the port is a root port or an alternate port. You cannot enable Loop Guard and Root Guard on a port at the same time. Loop Guard has no effect on a disabled spanning tree instance or a VLAN. Spanning tree always chooses the first operational port in the channel to send the BPDUs. If that link becomes unidirectional, Loop Guard blocks the channel, even if other links in the channel are functioning properly. If you group a set of ports that are already blocked by Loop Guard to form a channel, spanning tree loses all the state information for those ports and the new channel port may obtain the forwarding state with a designated role. If a channel is blocked by Loop Guard and the channel members go back to an individual link status, spanning tree loses all the state information. The individual physical ports may obtain the forwarding state with the designated role, even if one or more of the links that formed the channel are unidirectional. <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide (2011), at 179.</p>	<p>Loop guard, when enabled globally, applies to all point-to-point ports. Loop guard is configurable on individual ports and applies to all STP instances of an enabled port. Loop-inconsistent ports transition to listening state when loop guard is disabled.</p> <p>Enabling loop guard on a root switch has no effect until the switch becomes a nonroot switch.</p> <p>When using loop guard:</p> <ul style="list-style-type: none"> Do not enable loop guard on portfast-enabled ports. Loop guard is not functional on ports not connected to point-to-point links. Loop guard has no effect on disabled spanning tree instances. <p>Loop guard aspects on port channels include:</p> <ul style="list-style-type: none"> BPDUs are sent over the channel's first operational port. Loop guard blocks the channel if that link becomes unidirectional even when other channel links function properly. Creating a new channel destroys state information for its component ports; new channels with loop-guard-enabled ports can enter forwarding state as a DP. Disassembling a channel destroys its state information; component ports from a blocked channel can enter the forwarding state as DPs, even if the channel contained unidirectional links. A unidirectional link on any port of a loop-guard-enabled channel blocks the entire channel until the affected port is removed or the link resumes bidirectional operation. <p>Loop guard configuration commands include:</p> <ul style="list-style-type: none"> <code>spanning-tree loopguard default</code> command enables loop guard as a default on all switch ports. <code>spanning-tree guard</code> control the loop guard setting on the configuration mode interface. This command overrides the default command for the specified interface. <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 966.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 844; Arista User Manual, v. 4.11.1 (1/11/13), at 662; Arista User Manual v. 4.10.3 (10/22/12), at 576; Arista User Manual v. 4.9.3.2 (5/3/12), at 496; Arista User Manual v. 4.8.2 (11/18/11), at 370; Arista User Manual v. 4.7.3 (7/18/11), at 245.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>BPDU Guard</p> <p>Enabling BPDU Guard shuts down that interface if a BPDU is received.</p> <p>You can configure BPDU Guard at the interface level. When configured at the interface level, BPDU Guard shuts the port down as soon as the port receives a BPDU, regardless of the port type configuration.</p> <p>When you configure BPDU Guard globally, it is effective only on operational spanning tree edge ports. In a valid configuration, Layer 2 LAN edge interfaces do not receive BPDUs. A BPDU that is received by an edge</p> <p>Layer 2 LAN interface signals an invalid configuration, such as the connection of an unauthorized device. BPDU Guard, when enabled globally, shuts down all spanning tree edge ports when they receive a BPDU. BPDU Guard provides a secure response to invalid configurations, because you must manually put the Layer 2 LAN interface back in service after an invalid configuration.</p> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide (2011), at 174-75.</p>	<p>20.3.4.3 BPDU Guard</p> <p>PortFast interfaces do not receive BPDUs in a valid configuration. BPDU Guard provides a secure response to invalid configurations by disabling ports when they receive a BPDU. Disabled ports differ from blocked ports in that they are re-enabled only through manual intervention.</p> <ul style="list-style-type: none"> When configured globally, BPDU Guard is enabled on ports in the operational portfast state. When configured on an individual interface, BPDU Guard disables the port when it receives a BPDU, regardless of the port's portfast state. <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 968.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 846; Arista User Manual, v. 4.11.1 (1/11/13), at 664-65; Arista User Manual v. 4.10.3 (10/22/12), at 578; Arista User Manual v. 4.9.3.2 (5/3/12), at 498; Arista User Manual v. 4.8.2 (11/18/11), at 372; Arista User Manual v. 4.7.3 (7/18/11), at 246.</p>
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>BPDU Filtering</p> <p>You can use BPDU Filtering to prevent the device from sending or even receiving BPDUs on specified ports.</p> <p>When configured globally, BPDU Filtering applies to all operational spanning tree edge ports. You should connect edge ports only to hosts, which typically drop BPDUs. If an operational spanning tree edge port receives a BPDU, it immediately returns to a normal spanning tree port type and moves through the regular transitions. In that case, BPDU Filtering is disabled on this port, and spanning tree resumes sending BPDUs on this port.</p> <p>In addition, you can configure BPDU Filtering by the individual interface. When you explicitly configure BPDU Filtering on a port, that port does not send any BPDUs and drops all BPDUs that it receives. You can effectively override the global BPDU Filtering setting on individual ports by configuring the specific interface. This BPDU Filtering command on the interface applies to the entire interface, whether the interface is trunking or not.</p> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide (2011), at 175.</p>	<p>20.3.4.4 BPDU Filter</p> <p>BPDU filtering prevents the switch from sending or receiving BPDUs on specified ports. BPDU filtering is configurable on Ethernet and port channel interfaces.</p> <p>Ports with BPDU filtering enabled do not send BPDUs and drops inbound BPDUs. Enabling BPDU filtering on a port not connected to a host can result in loops as the port continues forwarding data while ignoring inbound BPDU packets.</p> <p>The <code>spanning-tree bpduguard</code> command controls BPDU filtering on the configuration mode interface. BPDU filtering is disabled by default.</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 968.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 846-47; Arista User Manual, v. 4.11.1 (1/11/13), at 665; Arista User Manual v. 4.10.3 (10/22/12), at 579; Arista User Manual v. 4.9.3.2 (5/3/12), at 498; Arista User Manual v. 4.8.2 (11/18/11), at 372; Arista User Manual v. 4.7.3 (7/18/11), at 246.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>Bridge Assurance</p> <p>You can use Bridge Assurance to protect against certain problems that can cause bridging loops in the network. Specifically, you use Bridge Assurance to protect against a unidirectional link failure or other software failure and a device that continues to forward data traffic when it is no longer running the spanning tree algorithm.</p> <p> Note Bridge Assurance is supported only by Rapid PVST+ and MST.</p> <p>Bridge Assurance is enabled by default and can only be disabled globally. Also, Bridge Assurance can be enabled only on spanning tree network ports that are point-to-point links. Finally, both ends of the link must have Bridge Assurance enabled. If the device on one side of the link has Bridge Assurance enabled and the device on the other side either does not support Bridge Assurance or does not have this feature enabled, the connecting port is blocked.</p> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide (2011), at 175.</p>	<p>spanning-tree bridge assurance</p> <p>The spanning-tree bridge assurance command enables bridge assurance on all ports with a port type of network. Bridge assurance protects against unidirectional link failure, other software failure, and devices that quit running a spanning tree algorithm.</p> <p>Bridge assurance is available only on spanning tree network ports on point-to-point links. Both ends of the link must have bridge assurance enabled. If the device on one side of the link has bridge assurance enabled and the device on the other side either does not support bridge assurance or does not have it enabled, the bridge assurance enabled port is blocked.</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1002.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 880; Arista User Manual, v. 4.11.1 (1/11/13), at 698; Arista User Manual v. 4.10.3 (10/22/12), at 612; Arista User Manual v. 4.9.3.2 (5/3/12), at 531; Arista User Manual v. 4.8.2 (11/18/11), at 403; Arista User Manual v. 4.7.3 (7/18/11), at 252.</p>
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<ul style="list-style-type: none"> • Root Guard—Root Guard prevents the port from becoming the root in an STP topology. <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide (2011), at 6.</p>	<ul style="list-style-type: none"> • Root guard prevents a port from becoming a root or blocked port. A root guard port that receives a superior BPDU transitions to the root-inconsistent (blocked) state. <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1005.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 883; Arista User Manual, v. 4.11.1 (1/11/13), at 701; Arista User Manual v. 4.10.3 (10/22/12), at 615; Arista User Manual v. 4.9.3.2 (5/3/12), at 534; Arista User Manual v. 4.8.2 (11/18/11), at 406; Arista User Manual v. 4.7.3 (7/18/11), at 268.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p> Note Do not disable spanning tree on a VLAN unless all switches and bridges in the VLAN have spanning tree disabled. You cannot disable spanning tree on some switches and bridges in a VLAN and leave it enabled on other switches and bridges in the VLAN. This action can have unexpected results because switches and bridges with spanning tree enabled will have incomplete information regarding the physical topology of the network.</p> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide (2011), at 108.</p>	<p>Important When disabling spanning tree on a VLAN, ensure that all switches and bridges in the network disable spanning tree for the same VLAN. Disabling spanning tree on a subset of switches and bridges in a VLAN may have unexpected results because switches and bridges running spanning tree will have incomplete information regarding the network's physical topology.</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1023.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 901; Arista User Manual, v. 4.11.1 (1/11/13), at 719; Arista User Manual v. 4.10.3 (10/22/12), at 633; Arista User Manual v. 4.9.3.2 (5/3/12), at 550; Arista User Manual v. 4.8.2 (11/18/11), at 422; Arista User Manual v. 4.7.3 (7/18/11), at 264.</p>
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>The software elects a router as the IGMP querier on a subnet if it has the lowest IP address. As long as a router continues to receive query messages from a router with a lower IP address, it resets a timer that is based on its querier timeout value. If the querier timer of a router expires, it becomes the designated querier. If that router later receives a host query message from a router with a lower IP address, it drops its role as the designated querier and sets its querier timer again.</p> <p>Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide (2012), at 20 .</p>	<p>The router with the lowest IP address on a subnet sends membership queries as the IGMP querier. When a router receives a membership query from a source with a lower IP address, it resets its query response timer. Upon timer expiry, the router begins sending membership queries. If the router subsequently receives a membership query from a router with a lower IP address, it stops sending membership queries and resets the query response timer.</p> <p>Arista User Manual v. 4v. 4.14.3F - Rev. 2 (10/2/14), at 1779.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1505; Arista User Manual, v. 4.11.1 (1/11/13), at 1205; Arista User Manual v. 4.10.3 (10/22/12), at 999; Arista User Manual v. 4.9.3.2 (5/3/12), at 757; Arista User Manual v. 4.8.2 (11/18/11), at 579; Arista User Manual v. 4.7.3 (7/18/11), at 459; Arista User Manual v. 4.6.0 (12/22/2010), at 309</p>

Copyright Registration Information	Cisco	Arista																												
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<table><tr><td>IGMP version</td><td>2</td></tr><tr><td>Startup query interval</td><td>30 seconds</td></tr><tr><td>Startup query count</td><td>2</td></tr><tr><td>Robustness value</td><td>2</td></tr><tr><td>Querier timeout</td><td>255 seconds</td></tr><tr><td>Query timeout</td><td>255 seconds</td></tr><tr><td>Query max response time</td><td>10 seconds</td></tr><tr><td>Query interval</td><td>125 seconds</td></tr><tr><td>Last member query response interval</td><td>1 second</td></tr><tr><td>Last member query count</td><td>2</td></tr><tr><td>Group membership timeout</td><td>260 seconds</td></tr><tr><td>Report link local multicast groups</td><td>Disabled</td></tr><tr><td>Enforce router alert</td><td>Disabled</td></tr><tr><td>Immediate leave</td><td>Disabled</td></tr></table>	IGMP version	2	Startup query interval	30 seconds	Startup query count	2	Robustness value	2	Querier timeout	255 seconds	Query timeout	255 seconds	Query max response time	10 seconds	Query interval	125 seconds	Last member query response interval	1 second	Last member query count	2	Group membership timeout	260 seconds	Report link local multicast groups	Disabled	Enforce router alert	Disabled	Immediate leave	Disabled	<div><p>Current IGMP router version: 2 IGMP query interval: 125 seconds IGMP max query response time: 100 deciseconds Last member query response interval: 10 deciseconds Last member query response count: 2 IGMP querier: 172.17.26.1 Robustness: 2 Require router alert: enabled Startup query interval: 312 deciseconds Startup query count: 2 General query timer expiry: 00:00:22 Multicast groups joined: 239.255.255.250</p></div> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1850.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1558; Arista User Manual, v. 4.11.1 (1/11/13), at 1253; Arista User Manual v. 4.10.3 (10/22/12), at 1038; Arista User Manual v. 4.9.3.2 (5/3/12), at 796; Arista User Manual v. 4.8.2 (11/18/11), at 614; Arista User Manual v. 4.7.3 (7/18/11), at 491; Arista User Manual v. 4.6.0 (12/22/2010), at 337.</p>
	IGMP version	2																												
	Startup query interval	30 seconds																												
	Startup query count	2																												
	Robustness value	2																												
	Querier timeout	255 seconds																												
	Query timeout	255 seconds																												
	Query max response time	10 seconds																												
	Query interval	125 seconds																												
	Last member query response interval	1 second																												
	Last member query count	2																												
	Group membership timeout	260 seconds																												
	Report link local multicast groups	Disabled																												
	Enforce router alert	Disabled																												
Immediate leave	Disabled																													
Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide (2012), at 24.																														

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>Anycast-RP</p> <p>Anycast-RP has two implementations: one uses Multicast Source Discovery Protocol (MSDP) and the other is based on <i>RFC 4610, Anycast-RP Using Protocol Independent Multicast (PIM)</i>. This section describes how to configure PIM Anycast-RP.</p> <p>You can use PIM Anycast-RP to assign a group of routers, called the Anycast-RP set, to a single RP address that is configured on multiple routers. The set of routers that you configure as Anycast-RPs is called the Anycast-RP set. This method is the only RP method that supports more than one RP per multicast group, which allows you to load balance across all RPs in the set. The Anycast RP supports all multicast groups.</p> <p>PIM register messages are sent to the closest RP and PIM join-prune messages are sent in the direction of the closest RP as determined by the unicast routing protocols. If one of the RPs goes down, unicast routing ensures these message will be sent in the direction of the next-closest RP.</p> <p>You must configure PIM on the loopback interface that is used for the PIM Anycast RP.</p> <p>For more information about PIM Anycast-RP, see <i>RFC 4610</i>.</p> <p>For information about configuring Anycast-RPs, see <i>Configuring a PIM Anycast-RP Set</i>.</p> <p>PIM Register Messages</p> <p>PIM register messages are unicast to the RP by designated routers (DRs) that are directly connected to multicast sources. The PIM register message has the following functions:</p> <ul style="list-style-type: none"> • To notify the RP that a source is actively sending to a multicast group. • To deliver multicast packets sent by the source to the RP for delivery down the shared tree. <p>The DR continues to send PIM register messages to the RP until it receives a Register-Stop message from the RP. The RP sends a Register-Stop message in either of the following cases:</p> <ul style="list-style-type: none"> • The RP has no receivers for the multicast group being transmitted. • The RP has joined the SPT to the source but has not started receiving traffic from the source. <p>Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide (2012), at 68-69.</p>	<p>Anycast-RP</p> <p>PIM Anycast-RP defines a single RP address that is configured on multiple routers. An anycast-RP set consists of the routers configured with the same anycast-RP address. Anycast-RP provides redundancy protection and load balancing. The anycast-RP set supports all multicast groups.</p> <p>PIM register messages are unicast to the RP by designated routers (DRs) that are directly connected to multicast sources. The switch sends these messages and join-prune messages to the anycast-RP set member specified in the anycast-RP command. In a typical configuration, one command is required for each member of the anycast-RP set.</p> <p>The PIM register message has the following functions:</p> <ul style="list-style-type: none"> • Notify the RP that a source is actively sending to a multicast group. • Deliver multicast packets sent by the source to the RP for delivery down the shared tree. <p>The DR continues sending PIM register messages to the RP until it receives a Register-Stop message from the RP. The RP sends a Register-Stop message in either of the following cases:</p> <ul style="list-style-type: none"> • The RP has no receivers for the multicast group being transmitted. • The RP has joined the SPT to the source but has not started receiving traffic from the source. <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1874.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1580; Arista User Manual, v. 4.11.1 (1/11/13), at 1274; Arista User Manual v. 4.10.3 (10/22/12), at 1005-06; Arista User Manual v. 4.9.3.2 (5/3/12), at 763-64; Arista User Manual v. 4.8.2 (11/18/11), at 639; Arista User Manual v. 4.7.3 (7/18/11), at 514.</p>
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>Note</p> <p>Use the show ip mroute command to display the statistics for multicast route and prefixes.</p> <p>Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide (2012), at 118.</p>	<p>Multicast Display Commands</p> <p>To display the information in the multicast routing table use the show ip mroute command. To display the MFIB table information, use the show ip mfib command.</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1758.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1486; Arista User Manual, v. 4.11.1 (1/11/13), at 1188; Arista User Manual v. 4.10.3 (10/22/12), at 1012; Arista User Manual v. 4.9.3.2 (5/3/12), at 770; Arista User Manual v. 4.8.2 (11/18/11), at 589; Arista User Manual v. 4.7.3 (7/18/11), at 469; Arista User Manual v. 4.6.0 (12/22/2010), at 319.</p>



Copyright Registration Information	Cisco	Arista												
Cisco IOS 12.4 Effective date of registration: 8/12/2005	<div>show ip mroute</div> <div>Displays the contents of the IP multicast routing table.</div> <div>Cisco IOS IP Multicast Command Reference (July 16, 2005), at 12.</div>	<div>Multicast Display Commands</div> <div>To display the information in the multicast routing table use the show ip mroute command. To display the MFIB table information, use the show ip mfib command.</div> <div>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1758</div> <div>See also Arista User Manual v. 4.12.3 (7/17/13), at 1486; Arista User Manual, v. 4.11.1 (1/11/13), at 1188; Arista User Manual v. 4.10.3 (10/22/12), at 1012; Arista User Manual v. 4.9.3.2 (5/3/12), at 770; Arista User Manual v. 4.8.2 (11/18/11), at 589; Arista User Manual v. 4.7.3 (7/18/11), at 469; Arista User Manual v. 4.6.0 (12/22/2010), at 319</div>												
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<table><tr><th>Command or Action</th><th>Purpose</th></tr><tr><td>Step 4</td><td></td></tr><tr><td><table><tr><th>Option</th><th>Description</th></tr><tr><td><div>ip igmp snooping</div><div>switch(config-vlan-config)# ip igmp snooping</div></td><td>Enables IGMP snooping for the current VLAN. The default is enabled.</td></tr><tr><td><div>ip igmp snooping explicit-tracking</div><div>switch(config-vlan-config)# ip igmp snooping explicit-tracking</div></td><td>Tracks IGMPv3 membership reports from individual hosts for each port on a per-VLAN basis. The default is enabled on all VLANs.</td></tr></table></td><td><div>These commands configure IGMP snooping parameters.</div></td></tr></table> <div>Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide (2012), at 139</div>	Command or Action	Purpose	Step 4		<table><tr><th>Option</th><th>Description</th></tr><tr><td><div>ip igmp snooping</div><div>switch(config-vlan-config)# ip igmp snooping</div></td><td>Enables IGMP snooping for the current VLAN. The default is enabled.</td></tr><tr><td><div>ip igmp snooping explicit-tracking</div><div>switch(config-vlan-config)# ip igmp snooping explicit-tracking</div></td><td>Tracks IGMPv3 membership reports from individual hosts for each port on a per-VLAN basis. The default is enabled on all VLANs.</td></tr></table>	Option	Description	<div>ip igmp snooping</div> <div>switch(config-vlan-config)# ip igmp snooping</div>	Enables IGMP snooping for the current VLAN. The default is enabled.	<div>ip igmp snooping explicit-tracking</div> <div>switch(config-vlan-config)# ip igmp snooping explicit-tracking</div>	Tracks IGMPv3 membership reports from individual hosts for each port on a per-VLAN basis. The default is enabled on all VLANs.	<div>These commands configure IGMP snooping parameters.</div>	<div>The ip igmp snooping command controls the global snooping setting. The ip igmp snooping vlan command enables snooping on individual VLANs if snooping is globally enabled. IGMP snooping is enabled on all VLANs by default.</div> <div>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1780</div> <div>See also Arista User Manual v. 4.12.3 (7/17/13), at 1506; Arista User Manual, v. 4.11.1 (1/11/13), at 1206; Arista User Manual v. 4.10.3 (10/22/12), at 998; Arista User Manual v. 4.9.3.2 (5/3/12), at 756; Arista User Manual v. 4.8.2 (11/18/11), at 581; Arista User Manual v. 4.7.3 (7/18/11), at 461.</div>
Command or Action	Purpose													
Step 4														
<table><tr><th>Option</th><th>Description</th></tr><tr><td><div>ip igmp snooping</div><div>switch(config-vlan-config)# ip igmp snooping</div></td><td>Enables IGMP snooping for the current VLAN. The default is enabled.</td></tr><tr><td><div>ip igmp snooping explicit-tracking</div><div>switch(config-vlan-config)# ip igmp snooping explicit-tracking</div></td><td>Tracks IGMPv3 membership reports from individual hosts for each port on a per-VLAN basis. The default is enabled on all VLANs.</td></tr></table>	Option	Description	<div>ip igmp snooping</div> <div>switch(config-vlan-config)# ip igmp snooping</div>	Enables IGMP snooping for the current VLAN. The default is enabled.	<div>ip igmp snooping explicit-tracking</div> <div>switch(config-vlan-config)# ip igmp snooping explicit-tracking</div>	Tracks IGMPv3 membership reports from individual hosts for each port on a per-VLAN basis. The default is enabled on all VLANs.	<div>These commands configure IGMP snooping parameters.</div>							
Option	Description													
<div>ip igmp snooping</div> <div>switch(config-vlan-config)# ip igmp snooping</div>	Enables IGMP snooping for the current VLAN. The default is enabled.													
<div>ip igmp snooping explicit-tracking</div> <div>switch(config-vlan-config)# ip igmp snooping explicit-tracking</div>	Tracks IGMPv3 membership reports from individual hosts for each port on a per-VLAN basis. The default is enabled on all VLANs.													
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<table><tr><td><div>ip igmp snooping mrouter interface interface</div><div>switch(config-vlan-config)# ip igmp snooping mrouter interface ethernet 2/1</div></td><td><div>Configures a static connection to a multicast router. The interface to the router must be in the selected VLAN. You can specify the interface by the type and the number, such as ethernet slot/port.</div></td></tr></table> <div>Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide (2012), at 140.</div>	<div>ip igmp snooping mrouter interface interface</div> <div>switch(config-vlan-config)# ip igmp snooping mrouter interface ethernet 2/1</div>	<div>Configures a static connection to a multicast router. The interface to the router must be in the selected VLAN. You can specify the interface by the type and the number, such as ethernet slot/port.</div>	<div>Specifying a Static Multicast Router Connection</div> <div>The ip igmp snooping vlan mrouter command statically configures a port that connects to a multicast router to join all multicast groups. The port to the router must be in the specified VLAN range.</div> <div>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1780</div> <div>See also Arista User Manual v. 4.12.3 (7/17/13), at 1506; Arista User Manual, v. 4.11.1 (1/11/13), at 1206; Arista User Manual v. 4.10.3 (10/22/12), at 1003; Arista User Manual v. 4.9.3.2 (5/3/12), at 761; Arista User Manual v. 4.8.2 (11/18/11), at 584; Arista User Manual v. 4.7.3 (7/18/11), at 503; Arista User Manual v. 4.6.0 (12/22/2010), at 349.</div>										
<div>ip igmp snooping mrouter interface interface</div> <div>switch(config-vlan-config)# ip igmp snooping mrouter interface ethernet 2/1</div>	<div>Configures a static connection to a multicast router. The interface to the router must be in the selected VLAN. You can specify the interface by the type and the number, such as ethernet slot/port.</div>													


Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>Displaying IGMP Snooping Statistics</p> <p>Use the <code>show ip igmp snooping statistics vlan</code> command to display IGMP snooping statistics. You can see the virtual port channel (vPC) statistics in this output.</p> <p>Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide (2012), at 144</p>	<p>show ip igmp statistics</p> <p>The <code>show ip igmp statistics</code> command displays IGMP transmission statistics for the specified interface.</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1867.</p>
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>SA Messages and Caching</p> <p>MSDP peers exchange Source-Active (SA) messages to propagate information about active sources. SA messages contain the following information:</p> <ul style="list-style-type: none"> • Source address of the data source • Group address that the data source uses • IP address of the RP or the configured originator ID <p>Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide (2012), at 148-49</p>	<p>35.2.2.1 Source Active Messages</p> <p>A Source Active (SA) message is a message that an RP creates and sends to MSDP peers when it learns of a new multicast source through a PIM register message. RPs that intend to originate or receive SA messages must establish MSDP peering with other RPs, either directly or through intermediate MSDP peers. An RP that is not a DR on a shared network should only originate SAs in response to register messages it receives from the DR. It does not originate SAs for directly connected sources in its domain.</p> <p>SA messages contain the following fields:</p> <ul style="list-style-type: none"> • Source address of the data source. • Group address that receives data sent by the source. • IP address of the RP <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1912.</p> <p>Arista User Manual v. 4.12.3 (7/17/13), at 1618; Arista User Manual, v. 4.11.1 (1/11/13), at 1310.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>RFC 5059</p> <p><i>Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)</i></p> <hr/> <p>Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide (2012), at 174.</p>	<p>34.3 Configuring PIM</p> <p>The following sections describe the configuration of static RPs, dynamic RPs, and anycast-RPs. RP implementation is defined through the following RFCs:</p> <ul style="list-style-type: none"> • RFC 5059: Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM). • RFC 6220: PIM Group-to-Rendezvous-Point Mapping. <p>This section describes the following configuration tasks:</p> <ul style="list-style-type: none"> • Section 34.3.1: Enabling PIM • Section 34.3.2: Rendezvous Points (RPs) • Section 34.3.3: Hello Messages • Section 34.3.4: Designated Router Election • Section 34.3.5: Join-Prune Messages <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1872.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1578; Arista User Manual, v. 4.11.1 (1/11/13), at 1272; Arista User Manual v. 4.10.3 (10/22/12), at 1004; Arista User Manual v. 4.9.3.2 (5/3/12), at 762.</p>
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>Audience</p> <p>This guide is for experienced network administrators who are responsible for configuring and maintaining the Cisco MDS 9000 Family of multilayer directors and fabric switches.</p> <p>Cisco DCNM Fundamentals Guide, Release 6.x (2011), at lxi.</p>	<p>Audience</p> <p>This guide is for experienced network administrators who are responsible for configuring and maintaining Arista switches.</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 41.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 35; Arista User Manual, v. 4.11.1 (1/11/13), at 29; Arista User Manual v. 4.10.3 (10/22/12), at 27; Arista User Manual v. 4.9.3.2 (5/3/12), at 23; Arista User Manual v. 4.8.2 (11/18/11), at 19; Arista User Manual v. 4.7.3 (7/18/11), at 17; Arista User Manual v. 4.6.0 (12/22/2010), at 13</p>

Copyright Registration Information	Cisco	Arista								
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<p>Table 5-1 Channel Modes for Individual Links in a Port Channel</p> <table><tr><th>Channel Mode</th><th>Description</th></tr><tr><td>passive</td><td>LACP mode that places a port into a passive negotiating state in which the port responds to LACP packets that it receives but does not initiate LACP negotiation.</td></tr><tr><td>active</td><td>LACP mode that places a port into an active negotiating state in which the port initiates negotiations with other ports by sending LACP packets.</td></tr><tr><td>on</td><td>All static port channels (that are not running LACP) remain in this mode. If you attempt to change the channel mode to active or passive before enabling LACP, the device displays an error message. You enable LACP on each channel by configuring the interface in that channel for the channel mode as either active or passive. When an LACP attempts to negotiate with an interface in the on state, it does not receive any LACP packets and becomes an individual link with that interface; it does not join the LACP channel group. The default port-channel mode is on.</td></tr></table> <p>Interfaces Configuration Guide, Cisco DCNM for LAN, Release 6.x (2012), at 5-10</p>	Channel Mode	Description	passive	LACP mode that places a port into a passive negotiating state in which the port responds to LACP packets that it receives but does not initiate LACP negotiation.	active	LACP mode that places a port into an active negotiating state in which the port initiates negotiations with other ports by sending LACP packets.	on	All static port channels (that are not running LACP) remain in this mode. If you attempt to change the channel mode to active or passive before enabling LACP, the device displays an error message. You enable LACP on each channel by configuring the interface in that channel for the channel mode as either active or passive. When an LACP attempts to negotiate with an interface in the on state, it does not receive any LACP packets and becomes an individual link with that interface; it does not join the LACP channel group. The default port-channel mode is on.	<p>Parameters</p> <ul style="list-style-type: none">number specifies a channel group ID. Values range from 1 through 1000.LACP_MODE specifies the interface LACP mode. Values include:<ul style="list-style-type: none">mode on Configures interface as a static port channel, disabling LACP. The switch does not verify or negotiate port channel membership with other switches.mode active Enables LACP on the interface in active negotiating state. The port initiates negotiations with other ports by sending LACP packets.mode passive Enables LACP on the interface in a passive negotiating state. The port responds to LACP packets but cannot start LACP negotiations. <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 469.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 403; Arista User Manual, v. 4.11.1 (1/11/13), at 336; Arista User Manual v. 4.10.3 (10/22/12), at 294; Arista User Manual v. 4.9.3.2 (5/3/12), at 278; Arista User Manual v. 4.8.2 (11/18/11), at 210; Arista User Manual v. 4.7.3 (7/18/11), at 424; Arista User Manual v. 4.6.0 (12/22/2010), at 271</p>
Channel Mode	Description									
passive	LACP mode that places a port into a passive negotiating state in which the port responds to LACP packets that it receives but does not initiate LACP negotiation.									
active	LACP mode that places a port into an active negotiating state in which the port initiates negotiations with other ports by sending LACP packets.									
on	All static port channels (that are not running LACP) remain in this mode. If you attempt to change the channel mode to active or passive before enabling LACP, the device displays an error message. You enable LACP on each channel by configuring the interface in that channel for the channel mode as either active or passive. When an LACP attempts to negotiate with an interface in the on state, it does not receive any LACP packets and becomes an individual link with that interface; it does not join the LACP channel group. The default port-channel mode is on.									
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<p>Table 6-1 Channel Modes for Individual Links in a Port Channel</p> <table><tr><th>Channel Mode</th><th>Description</th></tr><tr><td>passive</td><td>LACP mode that places a port into a passive negotiating state in which the port responds to LACP packets that it receives but does not initiate LACP negotiation.</td></tr><tr><td>active</td><td>LACP mode that places a port into an active negotiating state in which the port initiates negotiations with other ports by sending LACP packets.</td></tr><tr><td>on</td><td>All static port channels (that are not running LACP) remain in this mode. If you attempt to change the channel mode to active or passive before enabling LACP, the device displays an error message. You enable LACP on each channel by configuring the interface in that channel for the channel mode as either active or passive. When an LACP attempts to negotiate with an interface in the on state, it does not receive any LACP packets and becomes an individual link with that interface; it does not join the LACP channel group. The default port-channel mode is on.</td></tr></table> <p>Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x (2013), at 6-10</p>	Channel Mode	Description	passive	LACP mode that places a port into a passive negotiating state in which the port responds to LACP packets that it receives but does not initiate LACP negotiation.	active	LACP mode that places a port into an active negotiating state in which the port initiates negotiations with other ports by sending LACP packets.	on	All static port channels (that are not running LACP) remain in this mode. If you attempt to change the channel mode to active or passive before enabling LACP, the device displays an error message. You enable LACP on each channel by configuring the interface in that channel for the channel mode as either active or passive. When an LACP attempts to negotiate with an interface in the on state, it does not receive any LACP packets and becomes an individual link with that interface; it does not join the LACP channel group. The default port-channel mode is on.	<ul style="list-style-type: none">LACP_MODE specifies the interface LACP mode. Values include:<ul style="list-style-type: none">mode on Configures interface as a static port channel, disabling LACP. The switch does not verify or negotiate port channel membership with other switches.mode active Enables LACP on the interface in active negotiating state. The port initiates negotiations with other ports by sending LACP packets.mode passive Enables LACP on the interface in a passive negotiating state. The port responds to LACP packets but cannot start LACP negotiations. <p>Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 469.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 403; Arista User Manual, v. 4.11.1 (1/11/13), at 336; Arista User Manual v. 4.10.3 (10/22/12), at 294; Arista User Manual v. 4.9.3.2 (5/3/12), at 278; Arista User Manual v. 4.8.2 (11/18/11), at 210; Arista User Manual v. 4.7.3 (7/18/11), at 424; Arista User Manual v. 4.6.0 (12/22/2010), at 271</p>
Channel Mode	Description									
passive	LACP mode that places a port into a passive negotiating state in which the port responds to LACP packets that it receives but does not initiate LACP negotiation.									
active	LACP mode that places a port into an active negotiating state in which the port initiates negotiations with other ports by sending LACP packets.									
on	All static port channels (that are not running LACP) remain in this mode. If you attempt to change the channel mode to active or passive before enabling LACP, the device displays an error message. You enable LACP on each channel by configuring the interface in that channel for the channel mode as either active or passive. When an LACP attempts to negotiate with an interface in the on state, it does not receive any LACP packets and becomes an individual link with that interface; it does not join the LACP channel group. The default port-channel mode is on.									

Copyright Registration Information	Cisco	Arista								
Cisco NX-OS 5.0 Effective date of registration: 11/13/2014	<p>Table 5-1 Channel Modes for Individual Links in a Port Channel</p> <table><tr><th>Channel Mode</th><th>Description</th></tr><tr><td>passive</td><td>LACP mode that places a port into a passive negotiating state in which the port responds to LACP packets that it receives but does not initiate LACP negotiation.</td></tr><tr><td>active</td><td>LACP mode that places a port into an active negotiating state in which the port initiates negotiations with other ports by sending LACP packets.</td></tr><tr><td>on</td><td>All static port channels (that are not running LACP) remain in this mode. If you attempt to change the channel mode to active or passive before enabling LACP, the device displays an error message. You enable LACP on each channel by configuring the interface in that channel for the channel mode as either active or passive. When an LACP attempts to negotiate with an interface in the on state, it does not receive any LACP packets and becomes an individual link with that interface; it does not join the LACP channel group. The default port-channel mode is on.</td></tr></table> <p>Interfaces Configuration Guide, Cisco DCNM for LAN, Release 5.x (2010), at 6-9</p>	Channel Mode	Description	passive	LACP mode that places a port into a passive negotiating state in which the port responds to LACP packets that it receives but does not initiate LACP negotiation.	active	LACP mode that places a port into an active negotiating state in which the port initiates negotiations with other ports by sending LACP packets.	on	All static port channels (that are not running LACP) remain in this mode. If you attempt to change the channel mode to active or passive before enabling LACP, the device displays an error message. You enable LACP on each channel by configuring the interface in that channel for the channel mode as either active or passive. When an LACP attempts to negotiate with an interface in the on state, it does not receive any LACP packets and becomes an individual link with that interface; it does not join the LACP channel group. The default port-channel mode is on.	<p>Parameters</p> <ul style="list-style-type: none">number specifies a channel group ID. Values range from 1 through 1000.LACP_MODE specifies the interface LACP mode. Values include:<ul style="list-style-type: none">mode on Configures interface as a static port channel, disabling LACP. The switch does not verify or negotiate port channel membership with other switches.mode active Enables LACP on the interface in active negotiating state. The port initiates negotiations with other ports by sending LACP packets.mode passive Enables LACP on the interface in a passive negotiating state. The port responds to LACP packets but cannot start LACP negotiations. <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 469.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 403; Arista User Manual, v. 4.11.1 (1/11/13), at 336; Arista User Manual v. 4.10.3 (10/22/12), at 294; Arista User Manual v. 4.9.3.2 (5/3/12), at 278; Arista User Manual v. 4.8.2 (11/18/11), at 210; Arista User Manual v. 4.7.3 (7/18/11), at 424; Arista User Manual v. 4.6.0 (12/22/2010), at 271</p>
Channel Mode	Description									
passive	LACP mode that places a port into a passive negotiating state in which the port responds to LACP packets that it receives but does not initiate LACP negotiation.									
active	LACP mode that places a port into an active negotiating state in which the port initiates negotiations with other ports by sending LACP packets.									
on	All static port channels (that are not running LACP) remain in this mode. If you attempt to change the channel mode to active or passive before enabling LACP, the device displays an error message. You enable LACP on each channel by configuring the interface in that channel for the channel mode as either active or passive. When an LACP attempts to negotiate with an interface in the on state, it does not receive any LACP packets and becomes an individual link with that interface; it does not join the LACP channel group. The default port-channel mode is on.									
Cisco NX-OS 5.0 Effective date of registration: 11/13/2014	<p>Table 5-1 Channel Modes for Individual Links in a Port Channel</p> <table><tr><th>Channel Mode</th><th>Description</th></tr><tr><td>passive</td><td>LACP mode that places a port into a passive negotiating state in which the port responds to LACP packets that it receives but does not initiate LACP negotiation.</td></tr><tr><td>active</td><td>LACP mode that places a port into an active negotiating state in which the port initiates negotiations with other ports by sending LACP packets.</td></tr><tr><td>on</td><td>All static port channels (that are not running LACP) remain in this mode. If you attempt to change the channel mode to active or passive before enabling LACP, the device displays an error message. You enable LACP on each channel by configuring the interface in that channel for the channel mode as either active or passive. When an LACP attempts to negotiate with an interface in the on state, it does not receive any LACP packets and becomes an individual link with that interface; it does not join the LACP channel group. The default port-channel mode is on.</td></tr></table> <p>Interfaces Configuration Guide, Cisco DCNM for LAN, Release 4.x (2008), at 5-9</p>	Channel Mode	Description	passive	LACP mode that places a port into a passive negotiating state in which the port responds to LACP packets that it receives but does not initiate LACP negotiation.	active	LACP mode that places a port into an active negotiating state in which the port initiates negotiations with other ports by sending LACP packets.	on	All static port channels (that are not running LACP) remain in this mode. If you attempt to change the channel mode to active or passive before enabling LACP, the device displays an error message. You enable LACP on each channel by configuring the interface in that channel for the channel mode as either active or passive. When an LACP attempts to negotiate with an interface in the on state, it does not receive any LACP packets and becomes an individual link with that interface; it does not join the LACP channel group. The default port-channel mode is on.	<p>Parameters</p> <ul style="list-style-type: none">number specifies a channel group ID. Values range from 1 through 1000.LACP_MODE specifies the interface LACP mode. Values include:<ul style="list-style-type: none">mode on Configures interface as a static port channel, disabling LACP. The switch does not verify or negotiate port channel membership with other switches.mode active Enables LACP on the interface in active negotiating state. The port initiates negotiations with other ports by sending LACP packets.mode passive Enables LACP on the interface in a passive negotiating state. The port responds to LACP packets but cannot start LACP negotiations. <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 469.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 403; Arista User Manual, v. 4.11.1 (1/11/13), at 336; Arista User Manual v. 4.10.3 (10/22/12), at 294; Arista User Manual v. 4.9.3.2 (5/3/12), at 278; Arista User Manual v. 4.8.2 (11/18/11), at 210; Arista User Manual v. 4.7.3 (7/18/11), at 424; Arista User Manual v. 4.6.0 (12/22/2010), at 271</p>
Channel Mode	Description									
passive	LACP mode that places a port into a passive negotiating state in which the port responds to LACP packets that it receives but does not initiate LACP negotiation.									
active	LACP mode that places a port into an active negotiating state in which the port initiates negotiations with other ports by sending LACP packets.									
on	All static port channels (that are not running LACP) remain in this mode. If you attempt to change the channel mode to active or passive before enabling LACP, the device displays an error message. You enable LACP on each channel by configuring the interface in that channel for the channel mode as either active or passive. When an LACP attempts to negotiate with an interface in the on state, it does not receive any LACP packets and becomes an individual link with that interface; it does not join the LACP channel group. The default port-channel mode is on.									



Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p> Note For information about configuring port channels and the Link Aggregation Control Protocol (LACP), see Chapter 5, "Configuring Port Channels."</p> <p>Interfaces Configuration Guide, Cisco DCNM for LAN, Release 6.x (2012), at 6-2</p>	<p>Port Channels and LACP</p> <hr/> <p>This chapter describes channel groups, port channels, port channel interfaces, and the Link Aggregation Control Protocol (LACP). This chapter contains the following sections:</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 469.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 391; Arista User Manual, v. 4.11.1 (1/11/13), at 329; Arista User Manual v. 4.10.3 (10/22/12), at 287; Arista User Manual v. 4.9.3.2 (5/3/12), at 271; Arista User Manual v. 4.8.2 (11/18/11), at 203.</p>
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p> Note For information about configuring port channels and the Link Aggregation Control Protocol (LACP), see Chapter 5, "Configuring Port Channels."</p> <p>Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x (2013), at 7-1</p>	<p>Port Channels and LACP</p> <hr/> <p>This chapter describes channel groups, port channels, port channel interfaces, and the Link Aggregation Control Protocol (LACP). This chapter contains the following sections:</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 469.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 391; Arista User Manual, v. 4.11.1 (1/11/13), at 329; Arista User Manual v. 4.10.3 (10/22/12), at 287; Arista User Manual v. 4.9.3.2 (5/3/12), at 271; Arista User Manual v. 4.8.2 (11/18/11), at 203.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 5.0</p> <p>Effective date of registration: 11/13/2014</p>	<p> Note For information about configuring port channels and the Link Aggregation Control Protocol (LACP), see Chapter 5, "Configuring Port Channels."</p> <p>Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 5.x (2010), at 7-1</p>	<h2 data-bbox="1192 293 1728 337">Port Channels and LACP</h2> <p data-bbox="1192 375 2032 418">This chapter describes channel groups, port channels, port channel interfaces, and the Link Aggregation Control Protocol (LACP). This chapter contains the following sections:</p> <p data-bbox="1171 464 1835 492">Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 469.</p> <p data-bbox="1171 529 2018 659"><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 391; Arista User Manual, v. 4.11.1 (1/11/13), at 329; Arista User Manual v. 4.10.3 (10/22/12), at 287; Arista User Manual v. 4.9.3.2 (5/3/12), at 271; Arista User Manual v. 4.8.2 (11/18/11), at 203.</p>
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<h3 data-bbox="317 708 533 735">Loopback Interfaces</h3> <p data-bbox="453 748 1136 824">A loopback interface is a virtual interface with a single endpoint that is always up. Any packet transmitted over a loopback interface is immediately received by this interface. Loopback interfaces emulate a physical interface. You can configure up to 1024 loopback interfaces per VDC, numbered 0 to 1023.</p> <p data-bbox="300 865 1098 925">Interfaces Configuration Guide, Cisco DCNM for LAN, Release 6.x (2012), at 4-4 .</p>	<h4 data-bbox="1178 708 1423 735">14.4.4 Loopback Ports</h4> <p data-bbox="1266 740 2022 824">A loopback interface is a virtual network interface implemented in software and does not connect to any hardware. Traffic sent to the loopback interface is immediately received on the sending interface. The switch provides loopback configuration mode for creating loopback interfaces and modifying their operating parameters.</p> <p data-bbox="1171 865 1835 893">Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 631.</p> <p data-bbox="1171 930 1965 1027"><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 500; Arista User Manual, v. 4.11.1 (1/11/13), at 397; Arista User Manual v. 4.10.3 (10/22/12), at 329.</p>
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<h3 data-bbox="306 1068 525 1096">Loopback Interfaces</h3> <p data-bbox="453 1109 1136 1185">A loopback interface is a virtual interface with a single endpoint that is always up. Any packet transmitted over a loopback interface is immediately received by this interface. Loopback interfaces emulate a physical interface. You can configure up to 1024 loopback interfaces per VDC, numbered 0 to 1023.</p> <p data-bbox="300 1226 1066 1286">Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x (2013), at 4-4</p>	<h4 data-bbox="1178 1073 1423 1101">14.4.4 Loopback Ports</h4> <p data-bbox="1266 1105 2022 1190">A loopback interface is a virtual network interface implemented in software and does not connect to any hardware. Traffic sent to the loopback interface is immediately received on the sending interface. The switch provides loopback configuration mode for creating loopback interfaces and modifying their operating parameters.</p> <p data-bbox="1171 1230 1835 1258">Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 631.</p> <p data-bbox="1171 1295 1965 1393"><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 500; Arista User Manual, v. 4.11.1 (1/11/13), at 397; Arista User Manual v. 4.10.3 (10/22/12), at 329.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 5.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>Loopback Interfaces</p> <p>A loopback interface is a virtual interface with a single endpoint that is always up. Any packet transmitted over a loopback interface is immediately received by this interface. Loopback interfaces emulate a physical interface. You can configure up to 1024 loopback interfaces per VDC, numbered 0 to 1023.</p> <p>Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 5.x (2010), at 4-4</p>	<p>14.4.4 Loopback Ports</p> <p>A loopback interface is a virtual network interface implemented in software and does not connect to any hardware. Traffic sent to the loopback interface is immediately received on the sending interface. The switch provides loopback configuration mode for creating loopback interfaces and modifying their operating parameters.</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 631.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 500; Arista User Manual, v. 4.11.1 (1/11/13), at 397; Arista User Manual v. 4.10.3 (10/22/12), at 329.</p>
<p>Cisco NX-OS 4.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>Loopback Interfaces</p> <p>A loopback interface is a virtual interface with a single endpoint that is always up. Any packet transmitted over a loopback interface is immediately received by this interface. Loopback interfaces emulate a physical interface. You can configure up to 1024 loopback interfaces per VDC, numbered 0 to 1023.</p> <p>Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 4.x (2010), at 4-3</p>	<p>14.4.4 Loopback Ports</p> <p>A loopback interface is a virtual network interface implemented in software and does not connect to any hardware. Traffic sent to the loopback interface is immediately received on the sending interface. The switch provides loopback configuration mode for creating loopback interfaces and modifying their operating parameters.</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 631.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 500; Arista User Manual, v. 4.11.1 (1/11/13), at 397; Arista User Manual v. 4.10.3 (10/22/12), at 329.</p>
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>Configuring a Maximum Number of MAC Addresses</p> <p>You can configure the maximum number of MAC addresses that can be learned or statically configured on interfaces that belong to a port profile.</p> <p>Interfaces Configuration Guide, Cisco DCNM for LAN, Release 6.x (2012), at 10-22</p>	<p>Port Security Configuration</p> <p>MAC security restricts input to a switched port by limiting the number and identity of MAC addresses that can access the port.</p> <p>MAC address security is enabled by switchport port-security. Ports with MAC security enabled restrict traffic to a limited number of hosts, as determined by their MAC addresses. The maximum number of MAC addresses that can be assigned to an interface is configured by switchport port-security maximum. The default MAC address limit on an interface where port security is enabled is one.</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 632.</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 624; Arista User Manual v. 4.12.3 (7/17/13), at 501; Arista User Manual, v. 4.11.1 (1/11/13), at 405; Arista User Manual v. 4.10.3 (10/22/12), at 336.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>By default, an interface can have only one secure MAC address. You can configure the maximum number of MAC addresses permitted per interface or per VLAN on an interface. Maximums apply to secure MAC addresses learned by any method: dynamic, sticky, or static.</p> <p>ICisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 6.x (2013), at 507</p>	<p>Port Security Configuration</p> <p>MAC security restricts input to a switched port by limiting the number and identity of MAC addresses that can access the port.</p> <p>MAC address security is enabled by switchport port-security. Ports with MAC security enabled restrict traffic to a limited number of hosts, as determined by their MAC addresses. The maximum number of MAC addresses that can be assigned to an interface is configured by switchport port-security maximum. The default MAC address limit on an interface where port security is enabled is one.</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 632.</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 624; Arista User Manual v. 4.12.3 (7/17/13), at 501; Arista User Manual, v. 4.11.1 (1/11/13), at 405; Arista User Manual v. 4.10.3 (10/22/12), at 336.</p>
<p>Cisco NX-OS 5.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>By default, an interface can have only one secure MAC address. You can configure the maximum number of MAC addresses permitted per interface or per VLAN on an interface. Maximums apply to secure MAC addresses learned by any method: dynamic, sticky, or static.</p> <p>Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 5.x (2010), at 177</p>	<p>Port Security Configuration</p> <p>MAC security restricts input to a switched port by limiting the number and identity of MAC addresses that can access the port.</p> <p>MAC address security is enabled by switchport port-security. Ports with MAC security enabled restrict traffic to a limited number of hosts, as determined by their MAC addresses. The maximum number of MAC addresses that can be assigned to an interface is configured by switchport port-security maximum. The default MAC address limit on an interface where port security is enabled is one.</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 632.</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 624; Arista User Manual v. 4.12.3 (7/17/13), at 501; Arista User Manual, v. 4.11.1 (1/11/13), at 405; Arista User Manual v. 4.10.3 (10/22/12), at 336.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>This example shows how to return to EXEC mode from global configuration mode:</p> <pre>switch(config)# end switch#</pre> <p>This example shows how to return to EXEC mode from interface configuration mode:</p> <pre>switch(config-if)# end switch#</pre> <p>Cisco Nexus 7000 Series NX-OS Fundamentals Command Reference (2013), at FND-44</p>	<ul style="list-style-type: none"> To return to Privileged EXEC mode from any configuration mode, type end or Ctrl-Z. <pre>switch(config-if-Et24) #<Ctrl-z> switch#</pre> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 120.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 99; Arista User Manual, v. 4.11.1 (1/11/13), at 69; Arista User Manual v. 4.10.3 (10/22/12), at 61; Arista User Manual v. 4.9.3.2 (5/3/12), at 57; Arista User Manual v. 4.8.2 (11/18/11), at 52; Arista User Manual v. 4.7.3 (7/18/11), at 47; Arista User Manual v. 4.6.0 (12/22/2010), at 41</p>
<p>Cisco NX-OS 5.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>This example shows how to return to EXEC mode from global configuration mode:</p> <pre>switch(config)# end switch#</pre> <p>This example shows how to return to EXEC mode from interface configuration mode:</p> <pre>switch(config-if)# end switch#</pre> <p>Cisco Nexus 7000 Series NX-OS Fundamentals Command Reference (2010), at FND-37</p>	<ul style="list-style-type: none"> To return to Privileged EXEC mode from any configuration mode, type end or Ctrl-Z. <pre>switch(config-if-Et24) #<Ctrl-z> switch#</pre> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 120.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 99; Arista User Manual, v. 4.11.1 (1/11/13), at 69; Arista User Manual v. 4.10.3 (10/22/12), at 61; Arista User Manual v. 4.9.3.2 (5/3/12), at 57; Arista User Manual v. 4.8.2 (11/18/11), at 52; Arista User Manual v. 4.7.3 (7/18/11), at 47; Arista User Manual v. 4.6.0 (12/22/2010), at 41</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p> Note The reload command does not save the running configuration. Use the <u>copy running-config startup-config</u> command to save the current configuration on the device.</p> <p>Cisco Nexus 7000 Series NX-OS Fundamentals Command Reference (2013), at FND-105</p>	<p>Step 8 Type write memory (or <u>copy running-config startup-config</u>) to save the new configuration to the <i>startup-config</i> file. See Section 3.5.4: Saving the Running Configuration Settings.</p> <pre>switch# write memory switch#</pre> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 60.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 52; Arista User Manual, v. 4.11.1 (1/11/13), at 44; Arista User Manual v. 4.10.3 (10/22/12), at 38; Arista User Manual v. 4.9.3.2 (5/3/12), at 34; Arista User Manual v. 4.8.2 (11/18/11), at 30; Arista User Manual v. 4.7.3 (7/18/11), at 28; Arista User Manual v. 4.6.0 (12/22/2010), at 25</p>
<p>Cisco NX-OS 5.0</p> <p>Effective date of registration: 11/13/2014</p>	<p> Note The reload command does not save the running configuration. Use the <u>copy running-config startup-config</u> command to save the current configuration on the device.</p> <p>Cisco Nexus 7000 Series NX-OS Fundamentals Command Reference (2010), at FND-84</p>	<p>Step 8 Type write memory (or <u>copy running-config startup-config</u>) to save the new configuration to the <i>startup-config</i> file. See Section 3.5.4: Saving the Running Configuration Settings.</p> <pre>switch# write memory switch#</pre> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 60.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 52; Arista User Manual, v. 4.11.1 (1/11/13), at 44; Arista User Manual v. 4.10.3 (10/22/12), at 38; Arista User Manual v. 4.9.3.2 (5/3/12), at 34; Arista User Manual v. 4.8.2 (11/18/11), at 30; Arista User Manual v. 4.7.3 (7/18/11), at 28; Arista User Manual v. 4.6.0 (12/22/2010), at 25</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>This example shows how to display commands related to Open Shortest Path First (OSPF) available in the loopback interface command mode:</p> <pre>switch(config)# interface loopback 0 switch(config-if)# show cli list ospf MODE if-loopback no ip ospf network point-to-point no ip ospf network</pre> <p>Cisco Nexus 7000 Series NX-OS Fundamentals Command Reference (2013), at FND-126</p>	<p>Command Syntax</p> <pre>ip ospf network point-to-point no ip ospf network default ip ospf network</pre> <p>Examples</p> <ul style="list-style-type: none"> These commands configure Ethernet interface 10 as a point-to-point link. <pre>switch(config)#interface ethernet 10 switch(config-if-Et10)#ip ospf network point-to-point switch(config-if-Et10)#</pre> This command restores Ethernet interface 10 as a broadcast link. <pre>switch(config-if-Et10)#no ip ospf network switch(config-if-Et10)#</pre> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1432.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1219; Arista User Manual, v. 4.11.1 (1/11/13), at 976; Arista User Manual v. 4.10.3 (10/22/12), at 806; Arista User Manual v. 4.9.3.2 (5/3/12), at 692; Arista User Manual v. 4.8.2 (11/18/11), at 465; Arista User Manual v. 4.7.3 (7/18/11), at 338.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 5.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>This example shows how to display commands related to Open Shortest Path First (OSPF) available in the loopback interface command mode:</p> <pre>switch(config)# interface loopback 0 switch(config-if)# show cli list ospf MODE if-loopback no ip ospf network point-to-point no ip ospf network</pre> <p>Cisco Nexus 7000 Series NX-OS Fundamentals Command Reference (2010), at FND-105</p>	<p>Command Syntax</p> <pre>ip ospf network point-to-point no ip ospf network default ip ospf network</pre> <p>Examples</p> <ul style="list-style-type: none"> These commands configure Ethernet interface 10 as a point-to-point link. <pre>switch(config)#interface ethernet 10 switch(config-if-Et10)#ip ospf network point-to-point switch(config-if-Et10)#</pre> This command restores Ethernet interface 10 as a broadcast link. <pre>switch(config-if-Et10)#no ip ospf network switch(config-if-Et10)#</pre> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1432.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1219; Arista User Manual, v. 4.11.1 (1/11/13), at 976; Arista User Manual v. 4.10.3 (10/22/12), at 806; Arista User Manual v. 4.9.3.2 (5/3/12), at 692; Arista User Manual v. 4.8.2 (11/18/11), at 465; Arista User Manual v. 4.7.3 (7/18/11), at 338.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>show startup-config</p> <p>To display the startup configuration use the <code>show startup-config</code> command.</p> <p><code>show startup-config [exclude component-list]</code></p> <p>Cisco Nexus 7000 Series NX-OS Fundamentals Command Reference (2013), at FND-154.</p>	<p>Example</p> <ul style="list-style-type: none"> Type <code>show startup-config</code> to display the startup configuration file. The response in the example is truncated to display only the ip route configured in Admin Username (page 58). <pre> switch#show startup-config ! Command: show startup-config ! Startup-config last modified at Wed Feb 19 08:34:31 2014 by admin ! <-----OUTPUT OMITTED FROM EXAMPLE-----> ! ip route 0.0.0.0/0 192.0.2.1 ! <-----OUTPUT OMITTED FROM EXAMPLE-----> end switch# </pre> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 123.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 102; Arista User Manual, v. 4.11.1 (1/11/13), at 72; Arista User Manual v. 4.10.3 (10/22/12), at 65; Arista User Manual v. 4.9.3.2 (5/3/12), at 59; Arista User Manual v. 4.8.2 (11/18/11), at 54; Arista User Manual v. 4.7.3 (7/18/11), at 49.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>show startup-config</p> <p>To display the startup configuration use the show startup-config command.</p> <p>show startup-config [exclude component-list]</p> <p>Cisco Nexus 7000 Series NX-OS Fundamentals Command Reference (2010), at FND-125.</p>	<p>Example</p> <ul style="list-style-type: none"> Type show startup-config to display the startup configuration file. The response in the example is truncated to display only the ip route configured in Admin Username (page 58). <pre> switch#show startup-config ! Command: show startup-config ! Startup-config last modified at Wed Feb 19 08:34:31 2014 by admin ! <-----OUTPUT OMITTED FROM EXAMPLE-----> ! ip route 0.0.0.0/0 192.0.2.1 ! <-----OUTPUT OMITTED FROM EXAMPLE-----> end switch# </pre> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 123.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 102; Arista User Manual, v. 4.11.1 (1/11/13), at 72; Arista User Manual v. 4.10.3 (10/22/12), at 65; Arista User Manual v. 4.9.3.2 (5/3/12), at 59; Arista User Manual v. 4.8.2 (11/18/11), at 54; Arista User Manual v. 4.7.3 (7/18/11), at 49.</p>
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>Enabling the Error-Disable Detection</p> <p>You can enable error-disable detection in an application. As a result, when a cause is detected on an interface, the interface is placed in an error-disabled state, which is an operational state that is similar to the link-down state.</p> <p>Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x (2013), at 2-24.</p>	<p>14.5.2 Errdisabled Ports</p> <p>The switch places an Ethernet or management interface in error-disabled state when it detects an error on the interface. Error-disabled is an operational state that is similar to link-down state. Conditions that error-disables an interface includes:</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 123.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 503.</p>
<p>Cisco NX-OS 5.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>Enabling the Error-Disable Detection</p> <p>You can enable error-disable detection in an application. As a result, when a cause is detected on an interface, the interface is placed in an error-disabled state, which is an operational state that is similar to the link-down state.</p> <p>Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 5.x (2011), at 2-22.</p>	<p>14.5.2 Errdisabled Ports</p> <p>The switch places an Ethernet or management interface in error-disabled state when it detects an error on the interface. Error-disabled is an operational state that is similar to link-down state. Conditions that error-disables an interface includes:</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 123.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 503.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>This example shows how to configure a Layer 2 trunk interface, assign the native VLAN and the allowed VLANs, and configure the device to tag the native VLAN traffic on the trunk interface:</p> <pre>switch# configure terminal switch(config)# interface ethernet 2/35 switch(config-if)# switchport switch(config-if)# switchport mode trunk switch(config-if)# switchport trunk native vlan 10 switch(config-if)# switchport trunk allowed vlan 5, 10 switch(config-if)# exit switch(config)# vlan dot1q tag native switch(config)#</pre> <p>Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x (2013), at 3-36.</p>	<p>The trunk group command is not additive to the allowed vlan command</p> <pre>interface ethernet 1 switchport mode trunk switchport trunk allowed vlan 10 switchport trunk group trunk30</pre> <p>Vlan 30 will not be permitted on the interface as it is not listed in the allowed vlan list.</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 767.</p>
<p>Cisco NX-OS 5.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>This example shows how to configure a Layer 2 trunk interface, assign the native VLAN and the allowed VLANs, and configure the device to tag the native VLAN traffic on the trunk interface:</p> <pre>switch# configure terminal switch(config)# interface ethernet 2/35 switch(config-if)# switchport switch(config-if)# switchport mode trunk switch(config-if)# switchport trunk native vlan 10 switch(config-if)# switchport trunk allowed vlan 5, 10 switch(config-if)# exit switch(config)# vlan dot1q tag native switch(config)#</pre> <p>Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 5.x (2011), at 3-23-24.</p>	<p>The trunk group command is not additive to the allowed vlan command</p> <pre>interface ethernet 1 switchport mode trunk switchport trunk allowed vlan 10 switchport trunk group trunk30</pre> <p>Vlan 30 will not be permitted on the interface as it is not listed in the allowed vlan list.</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 767.</p>
<p>Cisco NX-OS 5.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>This example shows how to configure a Layer 2 trunk interface, assign the native VLAN and the allowed VLANs, and configure the device to tag the native VLAN traffic on the trunk interface:</p> <pre>switch# configure terminal switch(config)# interface ethernet 2/35 switch(config-if)# switchport switch(config-if)# switchport mode trunk switch(config-if)# switchport trunk native vlan 10 switch(config-if)# switchport trunk allowed vlan 5, 10 switch(config-if)# exit switch(config)# vlan dot1q tag native switch(config)#</pre> <p>Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 5.x (2010), at 3-19.</p>	<p>The trunk group command is not additive to the allowed vlan command</p> <pre>interface ethernet 1 switchport mode trunk switchport trunk allowed vlan 10 switchport trunk group trunk30</pre> <p>Vlan 30 will not be permitted on the interface as it is not listed in the allowed vlan list.</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 767.</p>

Copyright Registration Information	Cisco	Arista		
Cisco NX-OS 4.0 Effective date of registration: 11/13/2014	<p>This example shows how to configure a Layer 2 trunk interface, assign the native VLAN and the allowed VLANs, and configure the device to tag the native VLAN traffic on the trunk interface:</p> <pre>switch# configure terminal switch(config)# interface ethernet 2/35 switch(config-if)# switchport switch(config-if)# switchport mode trunk switch(config-if)# switchport trunk native vlan 10 switch(config-if)# switchport trunk allowed vlan 5, 10 switch(config-if)# exit switch(config)# vlan dot1q tag native switch(config)#</pre> <p>Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 5.x (2008), at 3-17.</p>	<p>The trunk group command is not additive to the allowed vlan command</p> <pre>interface ethernet 1 switchport mode trunk switchport trunk allowed vlan 10 switchport trunk group trunk30</pre> <p>Vlan 30 will not be permitted on the interface as it is not listed in the allowed vlan list.</p> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 767.</p>		
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<table><tr><td><pre>end</pre><p>Example:</p><pre>switch(config-router-af)# end</pre></td><td>Exits address family configuration mode and returns to global configuration mode.</td></tr></table> <p>Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x (2013), at 5-30.</p>	<pre>end</pre> <p>Example:</p> <pre>switch(config-router-af)# end</pre>	Exits address family configuration mode and returns to global configuration mode.	<ul style="list-style-type: none">This command exits server-failure configuration mode and returns to global configuration mode. <pre>switch(config-server-failure)#exit switch(config)#</pre> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 640.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 508.</p>
<pre>end</pre> <p>Example:</p> <pre>switch(config-router-af)# end</pre>	Exits address family configuration mode and returns to global configuration mode.			
Cisco IOS 15.0 Effective date of registration: 11/28/2014	<table><tr><td><pre>end</pre><p>Example:</p><pre>switch(config-router-af)# end</pre></td><td>Exits address family configuration mode and returns to global configuration mode.</td></tr></table> <p>Cisco IOS IP Multicast Configuration Guide (2009), at 289.</p>	<pre>end</pre> <p>Example:</p> <pre>switch(config-router-af)# end</pre>	Exits address family configuration mode and returns to global configuration mode.	<ul style="list-style-type: none">This command exits server-failure configuration mode and returns to global configuration mode. <pre>switch(config-server-failure)#exit switch(config)#</pre> <p>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 640.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 508.</p>
<pre>end</pre> <p>Example:</p> <pre>switch(config-router-af)# end</pre>	Exits address family configuration mode and returns to global configuration mode.			

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>Configuring the LACP Fast Timer Rate</p> <p>You can change the LACP timer rate to modify the duration of the LACP timeout. Use the <code>lacp rate</code> command to set the rate at which LACP control packets are sent to an LACP-supported interface. You can change the timeout rate from the default rate (30 seconds) to the fast rate (1 second). This command is supported only on LACP-enabled interfaces.</p> <p>Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x (2013), at 6-38,</p>	<p>lacp rate</p> <p>The <code>lacp rate</code> command configures the LACP transmission interval on the configuration mode interface. The LACP timeout sets the rate at which LACP control packets are sent to an LACP-supported interface.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 478.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 395; Arista User Manual, v. 4.11.1 (1/11/13), at 340; Arista User Manual v. 4.10.3 (10/22/12), at 298; Arista User Manual v. 4.9.3.2 (5/3/12), at 275; Arista User Manual v. 4.8.2 (11/18/11), at 213.</p>
<p>Cisco NX-OS 5.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>Configuring the LACP Fast Timer Rate</p> <p>You can change the LACP timer rate to modify the duration of the LACP timeout. Use the <code>lacp rate</code> command to set the rate at which LACP control packets are sent to an LACP-supported interface. You can change the timeout rate from the default rate (30 seconds) to the fast rate (1 second). This command is supported only on LACP-enabled interfaces.</p> <p>Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 5.x (June 14, 2011), at 6-333.</p>	<p>lacp rate</p> <p>The <code>lacp rate</code> command configures the LACP transmission interval on the configuration mode interface. The LACP timeout sets the rate at which LACP control packets are sent to an LACP-supported interface.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 478.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 395; Arista User Manual, v. 4.11.1 (1/11/13), at 340; Arista User Manual v. 4.10.3 (10/22/12), at 298; Arista User Manual v. 4.9.3.2 (5/3/12), at 275; Arista User Manual v. 4.8.2 (11/18/11), at 213.</p>

Copyright Registration Information	Cisco	Arista			
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<table border="1"> <tr> <td data-bbox="304 280 367 300">Step 3</td><td data-bbox="367 280 640 381"> <p>lacp rate fast</p> <p>Example: switch(config-if)# lacp rate fast</p> </td><td data-bbox="640 280 1144 381"> <p>Configures the fast rate (one second) at which LACP control packets are sent to an LACP-supported interface.</p> <p>To reset the timeout rate to its default, use the no form of the command.</p> </td></tr> </table> <p>Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x (2013), at 6-38.</p>	Step 3	<p>lacp rate fast</p> <p>Example: switch(config-if)# lacp rate fast</p>	<p>Configures the fast rate (one second) at which LACP control packets are sent to an LACP-supported interface.</p> <p>To reset the timeout rate to its default, use the no form of the command.</p>	<p>lacp rate</p> <p>The lacp rate command configures the LACP transmission interval on the configuration mode interface. The LACP timeout sets the rate at which LACP control packets are sent to an LACP-supported interface. Supported values include:</p> <ul style="list-style-type: none"> • <i>normal</i>: 30 seconds with synchronized interfaces; one second while interfaces are synchronizing. • <i>fast</i>: one second. <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 478.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 395; Arista User Manual, v. 4.11.1 (1/11/13), at 340; Arista User Manual v. 4.10.3 (10/22/12), at 298; Arista User Manual v. 4.9.3.2 (5/3/12), at 275; Arista User Manual v. 4.8.2 (11/18/11), at 213.</p>
Step 3	<p>lacp rate fast</p> <p>Example: switch(config-if)# lacp rate fast</p>	<p>Configures the fast rate (one second) at which LACP control packets are sent to an LACP-supported interface.</p> <p>To reset the timeout rate to its default, use the no form of the command.</p>			
<p>Cisco NX-OS 5.2</p> <p>Effective date of registration: 11/13/2014</p>	<table border="1"> <tr> <td data-bbox="304 743 367 763">Step 3</td><td data-bbox="367 743 640 844"> <p>lacp rate fast</p> <p>Example: switch(config-if)# lacp rate fast</p> </td><td data-bbox="640 743 1144 844"> <p>Configures the fast rate (one second) at which LACP control packets are sent to an LACP-supported interface.</p> <p>To reset the timeout rate to its default, use the no form of the command.</p> </td></tr> </table> <p>Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 5.x (June 14, 2011), at 6-34.</p>	Step 3	<p>lacp rate fast</p> <p>Example: switch(config-if)# lacp rate fast</p>	<p>Configures the fast rate (one second) at which LACP control packets are sent to an LACP-supported interface.</p> <p>To reset the timeout rate to its default, use the no form of the command.</p>	<p>lacp rate</p> <p>The lacp rate command configures the LACP transmission interval on the configuration mode interface. The LACP timeout sets the rate at which LACP control packets are sent to an LACP-supported interface. Supported values include:</p> <ul style="list-style-type: none"> • <i>normal</i>: 30 seconds with synchronized interfaces; one second while interfaces are synchronizing. • <i>fast</i>: one second. <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 478.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 395; Arista User Manual, v. 4.11.1 (1/11/13), at 340; Arista User Manual v. 4.10.3 (10/22/12), at 298; Arista User Manual v. 4.9.3.2 (5/3/12), at 275; Arista User Manual v. 4.8.2 (11/18/11), at 213.</p>
Step 3	<p>lacp rate fast</p> <p>Example: switch(config-if)# lacp rate fast</p>	<p>Configures the fast rate (one second) at which LACP control packets are sent to an LACP-supported interface.</p> <p>To reset the timeout rate to its default, use the no form of the command.</p>			

Copyright Registration Information	Cisco	Arista																	
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<table><tr><td>Syntax Description</td><td><table><tr><td>ipv4</td><td>(Optional) Configures BFD session parameters for the IPv4 address.</td></tr><tr><td>ipv6</td><td>(Optional) Configures BFD session parameters for the IPv6 address.</td></tr><tr><td>min_tx</td><td>Rate at which BFD control packets are sent to BFD neighbors. The configurable range is from 50 to 999.</td></tr><tr><td>min_rx msec</td><td>Specifies the rate at which BFD control packets are expected to be received from BFD neighbors. The range is from 50 to 999.</td></tr><tr><td>multiplier value</td><td>Specifies the number of consecutive BFD control packets that must be missed from a BFD neighbor before BFD declares that the neighbor is unavailable and the BFD neighbor is informed of the failure. The range is from 1 to 50.</td></tr></table></td></tr><tr><td>Defaults</td><td><table><tr><td>BFD interval: 50 milliseconds</td></tr><tr><td>min_rx: 50 milliseconds</td></tr><tr><td>multiplier: 3</td></tr></table></td></tr></table> Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, Release 6.x (2013), at 1-12.	Syntax Description	<table><tr><td>ipv4</td><td>(Optional) Configures BFD session parameters for the IPv4 address.</td></tr><tr><td>ipv6</td><td>(Optional) Configures BFD session parameters for the IPv6 address.</td></tr><tr><td>min_tx</td><td>Rate at which BFD control packets are sent to BFD neighbors. The configurable range is from 50 to 999.</td></tr><tr><td>min_rx msec</td><td>Specifies the rate at which BFD control packets are expected to be received from BFD neighbors. The range is from 50 to 999.</td></tr><tr><td>multiplier value</td><td>Specifies the number of consecutive BFD control packets that must be missed from a BFD neighbor before BFD declares that the neighbor is unavailable and the BFD neighbor is informed of the failure. The range is from 1 to 50.</td></tr></table>	ipv4	(Optional) Configures BFD session parameters for the IPv4 address.	ipv6	(Optional) Configures BFD session parameters for the IPv6 address.	min_tx	Rate at which BFD control packets are sent to BFD neighbors. The configurable range is from 50 to 999.	min_rx msec	Specifies the rate at which BFD control packets are expected to be received from BFD neighbors. The range is from 50 to 999.	multiplier value	Specifies the number of consecutive BFD control packets that must be missed from a BFD neighbor before BFD declares that the neighbor is unavailable and the BFD neighbor is informed of the failure. The range is from 1 to 50.	Defaults	<table><tr><td>BFD interval: 50 milliseconds</td></tr><tr><td>min_rx: 50 milliseconds</td></tr><tr><td>multiplier: 3</td></tr></table>	BFD interval: 50 milliseconds	min_rx: 50 milliseconds	multiplier: 3	<p>31.3.1 Configuring BFD on an Interface</p> <p>The transmission rate for BFD control packets, the minimum rate at which control packets are expected from the peer, and the multiplier (the number of packets that must be missed in succession before BFD declares the session to be down) are all configured per interface. These values apply to all BFD sessions that pass through the interface.</p> <p>The default values for these parameters are:</p> <ul style="list-style-type: none">• transmission rate 300 milliseconds• minimum receive rate 300 milliseconds• multiplier 3 <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1737.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1467.</p>
Syntax Description	<table><tr><td>ipv4</td><td>(Optional) Configures BFD session parameters for the IPv4 address.</td></tr><tr><td>ipv6</td><td>(Optional) Configures BFD session parameters for the IPv6 address.</td></tr><tr><td>min_tx</td><td>Rate at which BFD control packets are sent to BFD neighbors. The configurable range is from 50 to 999.</td></tr><tr><td>min_rx msec</td><td>Specifies the rate at which BFD control packets are expected to be received from BFD neighbors. The range is from 50 to 999.</td></tr><tr><td>multiplier value</td><td>Specifies the number of consecutive BFD control packets that must be missed from a BFD neighbor before BFD declares that the neighbor is unavailable and the BFD neighbor is informed of the failure. The range is from 1 to 50.</td></tr></table>	ipv4	(Optional) Configures BFD session parameters for the IPv4 address.	ipv6	(Optional) Configures BFD session parameters for the IPv6 address.	min_tx	Rate at which BFD control packets are sent to BFD neighbors. The configurable range is from 50 to 999.	min_rx msec	Specifies the rate at which BFD control packets are expected to be received from BFD neighbors. The range is from 50 to 999.	multiplier value	Specifies the number of consecutive BFD control packets that must be missed from a BFD neighbor before BFD declares that the neighbor is unavailable and the BFD neighbor is informed of the failure. The range is from 1 to 50.								
ipv4	(Optional) Configures BFD session parameters for the IPv4 address.																		
ipv6	(Optional) Configures BFD session parameters for the IPv6 address.																		
min_tx	Rate at which BFD control packets are sent to BFD neighbors. The configurable range is from 50 to 999.																		
min_rx msec	Specifies the rate at which BFD control packets are expected to be received from BFD neighbors. The range is from 50 to 999.																		
multiplier value	Specifies the number of consecutive BFD control packets that must be missed from a BFD neighbor before BFD declares that the neighbor is unavailable and the BFD neighbor is informed of the failure. The range is from 1 to 50.																		
Defaults	<table><tr><td>BFD interval: 50 milliseconds</td></tr><tr><td>min_rx: 50 milliseconds</td></tr><tr><td>multiplier: 3</td></tr></table>	BFD interval: 50 milliseconds	min_rx: 50 milliseconds	multiplier: 3															
BFD interval: 50 milliseconds																			
min_rx: 50 milliseconds																			
multiplier: 3																			
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<p>ip pim bfd-instance</p> <p>To enable Bidirectional Forwarding Detection (BFD) for Protocol Independent Multicast (PIM) on an interface, use the ip pim bfd-instance command. To return to the default setting, use the no form of this command.</p> <pre>ip pim bfd-instance [disable] no ip pim bfd-instance [disable]</pre> Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, Release 6.x (2013), at 1-251.	<p>31.3.2 Configuring BFD for PIM</p> <p>To enable or disable bidirectional forwarding detection (BFD) globally for all protocol independent multicast (PIM) neighbors, use the ip pim bfd command.</p> <p>To enable or disable PIM BFD on a specific interface, use the ip pim bfd-instance command. The interface-level configuration supercedes the global setting.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 766.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1467.</p>																	
Cisco NX-OS 5.0 Effective date of registration: 11/13/2014	<p>ip pim bfd-instance</p> <p>To enable Bidirectional Forwarding Detection (BFD) for Protocol Independent Multicast (PIM) on an interface, use the ip pim bfd-instance command. To return to the default setting, use the no form of this command.</p> <pre>ip pim bfd-instance [disable] no ip pim bfd-instance [disable]</pre> Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, Release 5.x (2010), at 66.	<p>31.3.2 Configuring BFD for PIM</p> <p>To enable or disable bidirectional forwarding detection (BFD) globally for all protocol independent multicast (PIM) neighbors, use the ip pim bfd command.</p> <p>To enable or disable PIM BFD on a specific interface, use the ip pim bfd-instance command. The interface-level configuration supercedes the global setting.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 766.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1467.</p>																	

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>switchport trunk native vlan</p> <p>To change the native VLAN ID when the interface is in trunking mode, use the switchport trunk native vlan command. To return the native VLAN ID to VLAN 1, use the no form of this command.</p> <p>switchport trunk native vlan <i>vlan-id</i></p> <p>no switchport trunk native vlan</p> <p>Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, Release 6.x (2013), at 1-253.</p>	<p>To specify the port's native VLAN, use the switchport trunk native vlan command.</p> <p>Example</p> <ul style="list-style-type: none"> These commands configure VLAN 12 as the native VLAN trunk for Ethernet interface 10. <pre>switch(config)#interface ethernet 10 switch(config-if-Et10)#switchport trunk native vlan 12 switch(config-if-Et10)#</pre> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 766.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 614; Arista User Manual, v. 4.11.1 (1/11/13), at 470; Arista User Manual v. 4.10.3 (10/22/12), at 390; Arista User Manual v. 4.9.3.2 (5/3/12), at 310.</p>
<p>Cisco NX-OS 5.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>switchport trunk native vlan</p> <p>i. switchport trunk native vlan command;</p> <p>To change the native VLAN ID when the interface is in trunking mode, use the switchport trunk native vlan command. To return the native VLAN ID to VLAN 1, use the no form of this command.</p> <p>switchport trunk native vlan <i>vlan-id</i></p> <p>no switchport trunk native vlan</p> <p>Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, Release 5.x (2010), at 222.</p>	<p>To specify the port's native VLAN, use the switchport trunk native vlan command.</p> <p>Example</p> <ul style="list-style-type: none"> These commands configure VLAN 12 as the native VLAN trunk for Ethernet interface 10. <pre>switch(config)#interface ethernet 10 switch(config-if-Et10)#switchport trunk native vlan 12 switch(config-if-Et10)#</pre> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 766.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 614; Arista User Manual, v. 4.11.1 (1/11/13), at 470; Arista User Manual v. 4.10.3 (10/22/12), at 390; Arista User Manual v. 4.9.3.2 (5/3/12), at 310.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 4.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>switchport trunk native vlan</p> <p>To change the native VLAN ID when the interface is in trunking mode, use the switchport trunk native vlan command. To return the native VLAN ID to VLAN 1, use the no form of this command.</p> <pre>switchport trunk native vlan vlan-id no switchport trunk native vlan</pre> <p>Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, Release 4.0 (2008), at IF-35.</p>	<p>To specify the port's native VLAN, use the switchport trunk native vlan command.</p> <p>Example</p> <ul style="list-style-type: none"> These commands configure VLAN 12 as the native VLAN trunk for Ethernet interface 10. <pre>switch(config)#interface ethernet 10 switch(config-if-Et10)#switchport trunk native vlan 12 switch(config-if-Et10)#</pre> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 766.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 614; Arista User Manual, v. 4.11.1 (1/11/13), at 470; Arista User Manual v. 4.10.3 (10/22/12), at 390; Arista User Manual v. 4.9.3.2 (5/3/12), at 310.</p>
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>This example shows how to clear all the dynamic Layer 2 entries from the MAC address table for VLAN 20 on port 2/20:</p> <pre>switch(config)#clear mac address-table dynamic vlan 20 interface ethernet 2/20 switch(config)#</pre> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, (2013), at 3.</p>	<p>Example</p> <ul style="list-style-type: none"> This command clears all dynamic mac address table entries for port channel 5 on VLAN 34. <pre>switch#clear mac address-table dynamic vlan 34 interface port-channel 5 switch#</pre> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 648.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 516; Arista User Manual, v. 4.11.1 (1/11/13), at 402; Arista User Manual v. 4.10.3 (10/22/12), at 333; Arista User Manual v. 4.9.3.2 (5/3/12), at 316.</p>
<p>Cisco NX-OS 5.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>This example shows how to clear all the dynamic Layer 2 entries from the MAC address table for VLAN 20 on port 2/20:</p> <pre>switch(config)#clear mac address-table dynamic vlan 20 interface ethernet 2/20 switch(config)#</pre> <p>Cisco NX-OS Layer 2 Switching Command Reference, Release 5.x (2010), at L2-2-L2-3.</p>	<p>Example</p> <ul style="list-style-type: none"> This command clears all dynamic mac address table entries for port channel 5 on VLAN 34. <pre>switch#clear mac address-table dynamic vlan 34 interface port-channel 5 switch#</pre> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 648.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 516; Arista User Manual, v. 4.11.1 (1/11/13), at 402; Arista User Manual v. 4.10.3 (10/22/12), at 333; Arista User Manual v. 4.9.3.2 (5/3/12), at 316.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 4.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>This example shows how to clear all the dynamic Layer 2 entries from the MAC address table for VLAN 20 on port 2/20:</p> <pre>switch(config)# clear mac address-table dynamic vlan 20 interface ethernet 2/20 switch(config)#</pre> <p>Cisco NX-OS Layer 2 Switching Command Reference, Release 4.0 (2008), at L2-2-L2-3.</p>	<p>Example</p> <ul style="list-style-type: none"> This command clears all dynamic mac address table entries for port channel 5 on VLAN 34. <pre>switch# clear mac address-table dynamic vlan 34 interface port-channel 5 switch#</pre> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 648.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 516; Arista User Manual, v. 4.11.1 (1/11/13), at 402; Arista User Manual v. 4.10.3 (10/22/12), at 333; Arista User Manual v. 4.9.3.2 (5/3/12), at 316.</p>
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p><u>Usage Guidelines</u> Rapid per VLAN Spanning Tree Plus (Rapid PVST+) and Multiple Spanning Tree (MST) have built-in compatibility mechanisms that allow them to interact properly with other versions of IEEE spanning tree or other regions. For example, a bridge running Rapid PVST+ can send 802.1D bridge protocol data units (BPDUs) on one of its ports when it is connected to a legacy bridge. An MST bridge can detect that a port is at the boundary of a region when it receives a legacy BPDU or an MST BPDU that is associated with a different region.</p> <p>Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, Release 6.x (2013), at 5.</p>	<p>20.2.1.4 Version Interoperability</p> <p>A network can contain switches running different spanning tree versions. The common spanning tree (CST) is a single forwarding path the switch calculates for STP, RSTP, MSTP, and Rapid-PVST topologies in networks containing multiple spanning tree variations.</p> <p>In multi-instance topologies, the following instances correspond to the CST</p> <ul style="list-style-type: none"> Rapid-PVST VLAN 1 MST IST (instance 0) <p>RSTP and MSTP are compatible with other spanning tree versions:</p> <ul style="list-style-type: none"> An RSTP bridge sends 802.1D (original STP) BPDUs on ports connected to an STP bridge. RSTP bridges operating in 802.1D mode remain in 802.1D mode even after all STP bridges are removed from their links. An MST bridge can detect that a port is at a region boundary when it receives an STP BPDU or an MST BPDU from a different region. MST ports assume they are boundary ports when the bridges to which they connect join the same region. <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 953.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 831; Arista User Manual, v. 4.11.1 (1/11/13), at 649; Arista User Manual v. 4.10.3 (10/22/12), at 563; Arista User Manual v. 4.9.3.2 (5/3/12), at 483; Arista User Manual v. 4.8.2 (11/18/11), at 357; Arista User Manual v. 4.7.3 (7/18/11), at 231.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 5.0</p> <p>Effective date of registration: 11/13/2014</p>	<p><u>Usage Guidelines</u> Rapid per VLAN Spanning Tree Plus (Rapid PVST+) and Multiple Spanning Tree (MST) have built-in compatibility mechanisms that allow them to interact properly with other versions of IEEE spanning tree or other regions. For example, a bridge running Rapid PVST+ can send 802.1D bridge protocol data units (BPDUs) on one of its ports when it is connected to a legacy bridge. An MST bridge can detect that a port is at the boundary of a region when it receives a legacy BPDU or an MST BPDU that is associated with a different region.</p> <p>Cisco NX-OS Layer 2 Switching Command Reference, Release 5.0 (2010), at L2-5.</p>	<p>20.2.1.4 Version Interoperability</p> <p>A network can contain switches running different spanning tree versions. The common spanning tree (CST) is a single forwarding path the switch calculates for STP, RSTP, MSTP, and Rapid-PVST topologies in networks containing multiple spanning tree variations.</p> <p>In multi-instance topologies, the following instances correspond to the CST:</p> <ul style="list-style-type: none"> • Rapid-PVST: VLAN 1 • MST IST (instance 0) <p>RSTP and MSTP are compatible with other spanning tree versions:</p> <ul style="list-style-type: none"> • An RSTP bridge sends 802.1D (original STP) BPDUs on ports connected to an STP bridge. • RSTP bridges operating in 802.1D mode remain in 802.1D mode even after all STP bridges are removed from their links. • An MST bridge can detect that a port is at a region boundary when it receives an STP BPDU or an MST BPDU from a different region. • MST ports assume they are boundary ports when the bridges to which they connect join the same region. <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 953.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 831; Arista User Manual, v. 4.11.1 (1/11/13), at 649; Arista User Manual v. 4.10.3 (10/22/12), at 563; Arista User Manual v. 4.9.3.2 (5/3/12), at 483; Arista User Manual v. 4.8.2 (11/18/11), at 357; Arista User Manual v. 4.7.3 (7/18/11), at 231.</p>

Copyright Registration Information	Cisco	Arista				
<div>Cisco NX-OS 4.0</div> <div>Effective date of registration: 11/13/2014</div>	<div><div>Usage Guidelines</div><div>Rapid per VLAN Spanning Tree Plus (Rapid PVST+) and Multiple Spanning Tree (MST) have built-in compatibility mechanisms that allow them to interact properly with other versions of IEEE spanning tree or other regions. For example, a bridge running Rapid PVST+ can send 802.1D bridge protocol data units (BPDUs) on one of its ports when it is connected to a legacy bridge. An MST bridge can detect that a port is at the boundary of a region when it receives a legacy BPDU or an MST BPDU that is associated with a different region.</div></div> <div>Cisco NX-OS Layer 2 Switching Command Reference, Release 4.0 (2008), at L2-5.</div>	<div>20.2.1.4 Version Interoperability</div> <div>A network can contain switches running different spanning tree versions. The common spanning tree (CST) is a single forwarding path the switch calculates for STP, RSTP, MSTP, and Rapid-PVST topologies in networks containing multiple spanning tree variations.</div> <div>In multi-instance topologies, the following instances correspond to the CST</div> <div><ul style="list-style-type: none">• Rapid-PVST: VLAN 1• MST IST (instance 0)</div> <div>RSTP and MSTP are compatible with other spanning tree versions:</div> <div><ul style="list-style-type: none">• An RSTP bridge sends 802.1D (original STP) BPDUs on ports connected to an STP bridge.• RSTP bridges operating in 802.1D mode remain in 802.1D mode even after all STP bridges are removed from their links.• An MST bridge can detect that a port is at a region boundary when it receives an STP BPDU or an MST BPDU from a different region.• MST ports assume they are boundary ports when the bridges to which they connect join the same region.</div> <div>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 953.</div> <div>See also Arista User Manual v. 4.12.3 (7/17/13), at 831; Arista User Manual, v. 4.11.1 (1/11/13), at 649; Arista User Manual v. 4.10.3 (10/22/12), at 563; Arista User Manual v. 4.9.3.2 (5/3/12), at 483; Arista User Manual v. 4.8.2 (11/18/11), at 357; Arista User Manual v. 4.7.3 (7/18/11), at 231.</div>				
<div>Cisco NX-OS 6.2</div> <div>Effective date of registration: 11/13/2014</div>	<div><div>Examples</div><div>This example shows how to add a static entry to the MAC address table:</div><div>switch(config)# mac address-table static 0050.3e8d.6400 vlan 3 interface ethernet 2/1 switch(config)#</div></div> <div><div>Related Commands</div><table><tr><th>Command</th><th>Description</th></tr><tr><td>show mac address-table</td><td>Displays information about the MAC address table.</td></tr></table></div> <div>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2013), at 20.</div>	Command	Description	show mac address-table	Displays information about the MAC address table.	<div>The mac address-table static command adds a static entry to the MAC address table.</div> <div>Example</div> <div><ul style="list-style-type: none">• This command adds a static entry for unicast MAC address 0012.3694.03ec to the MAC address table.<div>switch(config)#mac address-table static 0012.3694.03ec vlan 3 interface Ethernet 7 switch(config)#show mac address-table static</div></div> <div>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 624.</div> <div>See also Arista User Manual v. 4.12.3 (7/17/13), at 494; Arista User Manual, v. 4.11.1 (1/11/13), at 427-28; Arista User Manual, v. 4.11.1 (1/11/13), at; Arista User Manual v. 4.10.3 (10/22/12), at 331; Arista User Manual v. 4.9.3.2 (5/3/12), at 321-22.</div>
Command	Description					
show mac address-table	Displays information about the MAC address table.					

Copyright Registration Information	Cisco	Arista				
Cisco NX-OS 5.0 Effective date of registration: 11/13/2014	<div>Examples</div> <div>This example shows how to add a static entry to the MAC address table:</div> <div>switch(config)# mac address-table static 0050.3e8d.6400 vlan 3 interface ethernet 2/1 switch(config)#</div> <div><div>Related Commands</div><table><tr><th>Command</th><th>Description</th></tr><tr><td>show mac address-table</td><td>Displays information about the MAC address table.</td></tr></table></div> <div>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 5.x (2010), at L2-18.</div>	Command	Description	show mac address-table	Displays information about the MAC address table.	<div>The mac address-table static command adds a static entry to the MAC address table.</div> <div>Example</div> <div><ul style="list-style-type: none">This command adds a static entry for unicast MAC address 0012.3694.03ec to the MAC address table.</div> <div>switch(config)#mac address-table static 0012.3694.03ec vlan 3 interface Ethernet 7 switch(config)#show mac address-table static</div> <div>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 624.</div> <div>See also Arista User Manual v. 4.12.3 (7/17/13), at 494; Arista User Manual, v. 4.11.1 (1/11/13), at 427-28; Arista User Manual, v. 4.11.1 (1/11/13), at; Arista User Manual v. 4.10.3 (10/22/12), at 331; Arista User Manual v. 4.9.3.2 (5/3/12), at 321-22.</div>
Command	Description					
show mac address-table	Displays information about the MAC address table.					
Cisco NX-OS 4.0 Effective date of registration: 11/13/2014	<div>Examples</div> <div>This example shows how to add a static entry to the MAC address table:</div> <div>switch(config)# mac address-table static 0050.3e8d.6400 vlan 3 interface ethernet 2/1 switch(config)#</div> <div><div>Related Commands</div><table><tr><th>Command</th><th>Description</th></tr><tr><td>show mac address-table</td><td>Displays information about the MAC address table.</td></tr></table></div> <div>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 4.0 (2008), at L2-13.</div>	Command	Description	show mac address-table	Displays information about the MAC address table.	<div>The mac address-table static command adds a static entry to the MAC address table.</div> <div>Example</div> <div><ul style="list-style-type: none">This command adds a static entry for unicast MAC address 0012.3694.03ec to the MAC address table.</div> <div>switch(config)#mac address-table static 0012.3694.03ec vlan 3 interface Ethernet 7 switch(config)#show mac address-table static</div> <div>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 624.</div> <div>See also Arista User Manual v. 4.12.3 (7/17/13), at 494; Arista User Manual, v. 4.11.1 (1/11/13), at 427-28; Arista User Manual, v. 4.11.1 (1/11/13), at; Arista User Manual v. 4.10.3 (10/22/12), at 331; Arista User Manual v. 4.9.3.2 (5/3/12), at 321-22.</div>
Command	Description					
show mac address-table	Displays information about the MAC address table.					

Copyright Registration Information	Cisco	Arista									
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<table border="1"> <thead> <tr> <th>Related Commands</th><th>Command</th><th>Description</th></tr> </thead> <tbody> <tr> <td></td><td>show spanning-tree mst configuration</td><td>Displays information about the MST protocol.</td></tr> <tr> <td></td><td>spanning-tree mst configuration</td><td>Enters MST configuration submode.</td></tr> </tbody> </table> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2013), at 24.</p>	Related Commands	Command	Description		show spanning-tree mst configuration	Displays information about the MST protocol.		spanning-tree mst configuration	Enters MST configuration submode.	<p>show spanning-tree mst configuration</p> <p>The show spanning-tree mst configuration command displays information about the MST region's VLAN-to-instance mapping. The command provides two display options:</p> <ul style="list-style-type: none"> • default displays a table that lists the instance to VLAN map. • digest displays the configuration digest. <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 991.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 869; Arista User Manual, v. 4.11.1 (1/11/13), at 687; Arista User Manual v. 4.10.3 (10/22/12), at 601; Arista User Manual v. 4.9.3.2 (5/3/12), at 520; Arista User Manual v. 4.8.2 (11/18/11), at 394; Arista User Manual v. 4.7.3 (7/18/11), at 283.</p>
Related Commands	Command	Description									
	show spanning-tree mst configuration	Displays information about the MST protocol.									
	spanning-tree mst configuration	Enters MST configuration submode.									
<p>Cisco NX-OS 5.0</p> <p>Effective date of registration: 11/13/2014</p>	<table border="1"> <thead> <tr> <th>Related Commands</th><th>Command</th><th>Description</th></tr> </thead> <tbody> <tr> <td></td><td>show spanning-tree mst configuration</td><td>Displays information about the MST protocol.</td></tr> <tr> <td></td><td>spanning-tree mst configuration</td><td>Enters MST configuration submode.</td></tr> </tbody> </table> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 5.x (2010), at L2-26.</p>	Related Commands	Command	Description		show spanning-tree mst configuration	Displays information about the MST protocol.		spanning-tree mst configuration	Enters MST configuration submode.	<p>show spanning-tree mst configuration</p> <p>The show spanning-tree mst configuration command displays information about the MST region's VLAN-to-instance mapping. The command provides two display options:</p> <ul style="list-style-type: none"> • default displays a table that lists the instance to VLAN map. • digest displays the configuration digest. <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 991.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 869; Arista User Manual, v. 4.11.1 (1/11/13), at 687; Arista User Manual v. 4.10.3 (10/22/12), at 601; Arista User Manual v. 4.9.3.2 (5/3/12), at 520; Arista User Manual v. 4.8.2 (11/18/11), at 394; Arista User Manual v. 4.7.3 (7/18/11), at 283.</p>
Related Commands	Command	Description									
	show spanning-tree mst configuration	Displays information about the MST protocol.									
	spanning-tree mst configuration	Enters MST configuration submode.									

Copyright Registration Information	Cisco	Arista									
<p>Cisco NX-OS 4.0</p> <p>Effective date of registration: 11/13/2014</p>	<table border="1"> <thead> <tr> <th>Related Commands</th><th>Command</th><th>Description</th></tr> </thead> <tbody> <tr> <td></td><td>show spanning-tree mst configuration</td><td>Displays information about the MST protocol.</td></tr> <tr> <td></td><td>spanning-tree mst configuration</td><td>Enters MST configuration submode.</td></tr> </tbody> </table> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 4.x (2008), at L2-17.</p>	Related Commands	Command	Description		show spanning-tree mst configuration	Displays information about the MST protocol.		spanning-tree mst configuration	Enters MST configuration submode.	<p>show spanning-tree mst configuration</p> <p>The show spanning-tree mst configuration command displays information about the MST region's VLAN-to-instance mapping. The command provides two display options:</p> <ul style="list-style-type: none"> • default displays a table that lists the instance to VLAN map. • digest displays the configuration digest. <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 991.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 869; Arista User Manual, v. 4.11.1 (1/11/13), at 687; Arista User Manual v. 4.10.3 (10/22/12), at 601; Arista User Manual v. 4.9.3.2 (5/3/12), at 520; Arista User Manual v. 4.8.2 (11/18/11), at 394; Arista User Manual v. 4.7.3 (7/18/11), at 283.</p>
Related Commands	Command	Description									
	show spanning-tree mst configuration	Displays information about the MST protocol.									
	spanning-tree mst configuration	Enters MST configuration submode.									
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>Examples</p> <p>This example shows how to display VTP interface switchport information on the device:</p> <pre>switch# show interface switchport Name: Ethernet8/11 Switchport: Enabled Switchport Monitor: Not enabled Operational Mode: trunk Access Mode VLAN: 1 (default) Trunking Native Mode VLAN: 1 (default) Trunking VLANs Enabled: 1,10,20-30 Pruning VLANs Enabled: 2-1001 Administrative private-vlan primary host-association: none Administrative private-vlan secondary host-association: none Administrative private-vlan primary mapping: none Administrative private-vlan secondary mapping: none Administrative private-vlan trunk native VLAN: none Administrative private-vlan trunk encapsulation: dot1q Administrative private-vlan trunk normal VLANs: none Administrative private-vlan trunk private VLANs: none Operational private-vlan: none switch#</pre> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2013), at 44.</p>	<p>Example</p> <ul style="list-style-type: none"> • These commands create the trunk mode allowed VLAN list of 6-10 for Ethernet interface 14, then verifies the VLAN list. <pre>switch(config)#interface ethernet 14 switch(config-if-Et14)#switchport trunk allowed vlan 6-10 switch(config-if-Et14)#show interfaces ethernet 14 switchport Name: Et14 Switchport: Enabled Administrative Mode: trunk Operational Mode: trunk Access Mode VLAN: 1 (inactive) Trunking Native Mode VLAN: 1 (inactive) Administrative Native VLAN tagging: disabled Trunking VLANs Enabled: 6-10 Trunk Groups: switch(config-if-Et14)#</pre> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 798.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 645; Arista User Manual, v. 4.11.1 (1/11/13), at 498; Arista User Manual v. 4.10.3 (10/22/12), at 416; Arista User Manual v. 4.9.3.2 (5/3/12), at 355.</p>									

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>Examples</p> <p>This example shows how to display information about the specified VLAN. This command displays statistical information gathered on the VLAN at 1-minute intervals:</p> <pre> Switch# show interface vlan 5 Vlan5 is administratively down, line protocol is down Hardware is etherSVI, address is 0000.0000.0000 MTU 1500 bytes, BW 1000000 kbit, DLY is 0sec, reliability 255/255, txload 1/255, rxload 1/255 Encapsulation ARPA, loopback not set Keepalive not supported ARP type: ARPA Last clearing of "show interface" counters 01:21:55 1 minute input rate 0 bytes/sec, 0 packets/sec 1 minute output rate 0 bytes/sec, 0 packets/sec L3 Switched: input: 0 pkts, 0 bytes - output: 0 pkts, 0 bytes L3 in Switched: ucast: 0 pkts, 0 bytes - mcast: 0 pkts, 0 bytes L3 out Switched: ucast: 0 pkts, 0 bytes - mcast: 0 pkts, 0 bytes </pre> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2013), at 49.</p>	<p>Example</p> <ul style="list-style-type: none"> This command display configuration and status information for Ethernet interface 1 and 2. <pre> switch>show interfaces ethernet 1-2 Ethernet1 is up, line protocol is up (connected) Hardware is Ethernet, address is 001c.2481.7647 (bia 001c.2481.7647) Description: mkt.1 MTU 9212 bytes, BW 10000000 Kbit Full-duplex 10Gb/s, auto negotiation: off Last clearing of "show interface" counters never 5 seconds input rate 33.5 Mbps (0.3% with framing), 846 packets/sec 5 seconds output rate 180 kbps (0.0% with framing), 55 packets/sec 76437268 packets input, 94280286608 bytes Received 2208 broadcasts, 73358 multicast 0 runts, 0 giants 0 input errors, 0 CRC, 0 alignment, 0 symbol 0 PAUSE input 6184281 packets output, 4071319140 bytes Sent 2209 broadcasts, 345754 multicast 0 output errors, 0 collisions 0 late collision, 0 deferred 0 PAUSE output </pre> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 437.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 371; Arista User Manual, v. 4.11.1 (1/11/13), at 312; Arista User Manual v. 4.10.3 (10/22/12), at 270; Arista User Manual v. 4.9.3.2 (5/3/12), at 252.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 5.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>Examples</p> <p>This example shows how to display information about the specified VLAN. This command displays statistical information gathered on the VLAN at 1-minute intervals:</p> <pre> Switch# show interface vlan 5 Vlan5 is administratively down, line protocol is down Hardware is etherSVI, address is 0000.0000.0000 MTU 1500 bytes, BW 1000000 kbit, DLY is 0 usec, reliability 255/255, txload 1/255, rxload 1/255 Encapsulation ARPA, loopback not set Keepalive not supported ARP type: ARPA Last clearing of "show interface" counters 01:21:55 1 minute input rate 0 bytes/sec, 0 packets/sec 1 minute output rate 0 bytes/sec, 0 packets/sec L3 Switched: Input: 0 pkts, 0 bytes - output: 0 pkts, 0 bytes L3 in Switched: ucast: 0 pkts, 0 bytes - mcast: 0 pkts, 0 bytes L3 out Switched: ucast: 0 pkts, 0 bytes - mcast: 0 pkts, 0 bytes </pre> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 5.x (2010), at 46.</p>	<p>Example</p> <ul style="list-style-type: none"> This command display configuration and status information for Ethernet interface 1 and 2. <pre> switch>show interfaces ethernet 1-2 Ethernet1 is up, line protocol is up (connected) Hardware is Ethernet, address is 001c.2481.7647 (bia 001c.2481.7647) Description: mkt.1 MTU 9212 bytes, BW 10000000 Kbit Full-duplex 10Gb/s, auto negotiation: off Last clearing of "show interface" counters never 5 seconds input rate 33.5 Mbps (0.3% with framing), 846 packets/sec 5 seconds output rate 180 kbps (0.0% with framing), 55 packets/sec 76437268 packets input, 94280286608 bytes Received 2208 broadcasts, 73358 multicast 0 runts, 0 giants 0 input errors, 0 CRC, 0 alignment, 0 symbol 0 PAUSE input 6184281 packets output, 4071319140 bytes Sent 2209 broadcasts, 345754 multicast 0 output errors, 0 collisions 0 late collision, 0 deferred 0 PAUSE output </pre> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 437.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 371; Arista User Manual, v. 4.11.1 (1/11/13), at 312; Arista User Manual v. 4.10.3 (10/22/12), at 270; Arista User Manual v. 4.9.3.2 (5/3/12), at 252.</p>
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>show mac address-table</p> <p>To display the information about the MAC address table use the show mac address-table command.</p> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2013), at 54.</p>	<p>14.3.2 Displaying the MAC Address Table</p> <p>The show mac address-table command displays the specified MAC address table entries.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 626.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 496; Arista User Manual, v. 4.11.1 (1/11/13), at 402; Arista User Manual v. 4.10.3 (10/22/12), at 360; Arista User Manual v. 4.9.3.2 (5/3/12), at 333.</p>

Copyright Registration Information	Cisco	Arista				
Cisco NX-OS 5.0 Effective date of registration: 11/13/2014	<p>show mac address-table</p> <p>To display the information about the MAC address table, use the show mac address-table command.</p> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2010), at L-51.</p>	<p>14.3.2 Displaying the MAC Address Table</p> <p>The show mac address-table command displays the specified MAC address table entries.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 626.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 496; Arista User Manual, v. 4.11.1 (1/11/13), at 402; Arista User Manual v. 4.10.3 (10/22/12), at 360; Arista User Manual v. 4.9.3.2 (5/3/12), at 333.</p>				
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<table><tr><th>Command</th><th>Description</th></tr><tr><td>mac address-table static</td><td>Adds static entries to the MAC address table or configures a static MAC address with IGMP snooping disabled for that address.</td></tr></table> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2013), at 40.</p>	Command	Description	mac address-table static	Adds static entries to the MAC address table or configures a static MAC address with IGMP snooping disabled for that address.	<p>mac address-table static</p> <p>The mac address-table static command adds a static entry to the MAC address table. Each table entry references a MAC address, a VLAN, and a list of layer 2 (Ethernet or port channel) ports. The table supports three entry types: unicast drop, unicast, and multicast.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 664</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 532; Arista User Manual, v. 4.11.1 (1/11/13), at 427.</p>
Command	Description					
mac address-table static	Adds static entries to the MAC address table or configures a static MAC address with IGMP snooping disabled for that address.					
Cisco NX-OS 5.0 Effective date of registration: 11/13/2014	<table><tr><th>Command</th><th>Description</th></tr><tr><td>mac address-table static</td><td>Adds static entries to the MAC address table or configures a static MAC address with IGMP snooping disabled for that address.</td></tr></table> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 5.x (2013), at L2-53.</p>	Command	Description	mac address-table static	Adds static entries to the MAC address table or configures a static MAC address with IGMP snooping disabled for that address.	<p>mac address-table static</p> <p>The mac address-table static command adds a static entry to the MAC address table. Each table entry references a MAC address, a VLAN, and a list of layer 2 (Ethernet or port channel) ports. The table supports three entry types: unicast drop, unicast, and multicast.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 664</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 532; Arista User Manual, v. 4.11.1 (1/11/13), at 427.</p>
Command	Description					
mac address-table static	Adds static entries to the MAC address table or configures a static MAC address with IGMP snooping disabled for that address.					

Copyright Registration Information	Cisco	Arista				
Cisco IOS 5.1 Effective date of registration: 11/28/2014	<table><tr><th>Command</th><th>Description</th></tr><tr><td>mac address-table static</td><td>Adds static entries to the MAC address table or configures a static MAC address with IGMP snooping disabled for that address.</td></tr></table> Cisco IOS Security Command Reference (2010), at SEC-2374.	Command	Description	mac address-table static	Adds static entries to the MAC address table or configures a static MAC address with IGMP snooping disabled for that address.	<div>mac address-table static</div> <p>The mac address-table static command adds a static entry to the MAC address table. Each table entry references a MAC address, a VLAN, and a list of layer 2 (Ethernet or pprt channel) ports. The table supports three entry types: unicast drop, unicast, and multicast.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 664</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 532; Arista User Manual, v. 4.11.1 (1/11/13), at 427.</p>
Command	Description					
mac address-table static	Adds static entries to the MAC address table or configures a static MAC address with IGMP snooping disabled for that address.					
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<table><tr><th>Command</th><th>Description</th></tr><tr><td>mac address-table aging-time</td><td>Configures the aging time for entries in the Layer 2 table.</td></tr></table> Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2013), at 57.	Command	Description	mac address-table aging-time	Configures the aging time for entries in the Layer 2 table.	<p>The mac address-table aging-time command configures the aging time for MAC address table dynamic entries. Aging time defines the period an entry is in the table, as measured from the most recent reception of a frame on the entry's VLAN from the specified MAC address. The switch removes entries when their presence in the MAC address table exceeds the aging time.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 662</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 496; Arista User Manual, v. 4.11.1 (1/11/13), at 426; Arista User Manual v. 4.10.3 (10/22/12), at 332; Arista User Manual v. 4.9.3.2 (5/3/12), at 320.</p>
Command	Description					
mac address-table aging-time	Configures the aging time for entries in the Layer 2 table.					
Cisco IOS 5.1 Effective date of registration: 11/28/201	<table><tr><th>Command</th><th>Description</th></tr><tr><td>mac address-table aging-time</td><td>Configures the aging time for entries in the Layer 2 table.</td></tr></table> Cisco IOS Security Command Reference (2010), at SEC-2374.	Command	Description	mac address-table aging-time	Configures the aging time for entries in the Layer 2 table.	<p>The mac address-table aging-time command configures the aging time for MAC address table dynamic entries. Aging time defines the period an entry is in the table, as measured from the most recent reception of a frame on the entry's VLAN from the specified MAC address. The switch removes entries when their presence in the MAC address table exceeds the aging time.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 662</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 496; Arista User Manual, v. 4.11.1 (1/11/13), at 426; Arista User Manual v. 4.10.3 (10/22/12), at 332; Arista User Manual v. 4.9.3.2 (5/3/12), at 320.</p>
Command	Description					
mac address-table aging-time	Configures the aging time for entries in the Layer 2 table.					

Copyright Registration Information	Cisco	Arista				
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<table><tr><th>Command</th><th>Description</th></tr><tr><td>mac address-table aging-time</td><td>Configures the aging time for entries in the Layer 2 table.</td></tr></table> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 5.x (2010), at L-54.</p>	Command	Description	mac address-table aging-time	Configures the aging time for entries in the Layer 2 table.	<p>The <code>mac address-table aging-time</code> command configures the aging time for MAC address table dynamic entries. Aging time defines the period an entry is in the table, as measured from the most recent reception of a frame on the entry's VLAN from the specified MAC address. The switch removes entries when their presence in the MAC address table exceeds the aging time.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 662</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 496; Arista User Manual, v. 4.11.1 (1/11/13), at 426; Arista User Manual v. 4.10.3 (10/22/12), at 332; Arista User Manual v. 4.9.3.2 (5/3/12), at 320.</p>
Command	Description					
mac address-table aging-time	Configures the aging time for entries in the Layer 2 table.					
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<p>Examples</p> <p>This example shows how to display STP when you are running Rapid PVST+:</p> <pre>Switch# show spanning-tree</pre> <pre>VLAN0001 Spanning tree enabled protocol rstp Root ID Priority 32768 Address 000d.eca3.9f01 Cost 4 Port 4105 (port-channel10) Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec Bridge ID Priority 32768 (priority 32768 sys-id-ext 1) Address 0022.5579.7641 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec Interface Role Sts Cost Prio.Nbr Type ----- Po10 Root FWD 2 128.4105 (vPC peer-link) P2p Po20 Desg FWD 1 128.4115 (vPC) P2p Po30 Root FWD 1 128.4125 (vPC) P2p</pre> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, (2013), at 63.</p>	<p>Show commands (such as <code>show spanning-tree</code>) displays the RSTP instance as MST0 (MST instance 0).</p> <p>Example</p> <ul style="list-style-type: none">This command, while the switch is in RST mode, displays RST instance information. <pre>switch(config)#show spanning-tree MST0 Spanning tree enabled protocol rstp Root ID Priority 32768 Address 001c.730c.1867 This bridge is the root Bridge ID Priority 32768 (priority 32768 sys-id-ext 0) Address 001c.730c.1867 Hello Time 2.000 sec Max Age 20 sec Forward Delay 15 sec Interface Role State Cost Prio.Nbr Type ----- Et51 designated forwarding 2000 128.51 P2p</pre> <p>switch(config)#</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 960.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 838; Arista User Manual, v. 4.11.1 (1/11/13), at 656; Arista User Manual v. 4.10.3 (10/22/12), at 570; Arista User Manual v. 4.9.3.2 (5/3/12), at 490; Arista User Manual v. 4.8.2 (11/18/11), at 364; Arista User Manual v. 4.7.3 (7/18/11), at 238; Arista User Manual v. 4.6.0 (12/22/2010), at 268.</p>				

Copyright Registration Information	Cisco	Arista																																																												
Cisco NX-OS 5.0 Effective date of registration: 11/13/2014	<p>Examples</p> <p>This example shows how to display STP when you are running Rapid PVST+:</p> <pre>switch# show spanning-tree</pre> <pre>VLAN0001 Spanning tree enabled protocol rstp Root ID Priority 32769 Address 000d.eca3.9f01 Cost 4 Port 4105 (port-channel10) Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec</pre> <pre>Bridge ID Priority 32769 (priority 32768 sys-id-ext 1) Address 0022.5579.7641 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec</pre> <table><thead><tr><th>Interface</th><th>Role</th><th>Sts</th><th>Cost</th><th>Prio.Nbr</th><th>Type</th></tr></thead><tbody><tr><td>Et10</td><td>Root</td><td>FWD</td><td>2</td><td>128.4105</td><td>(vpc peer-link) P2p</td></tr><tr><td>Et20</td><td>Desig</td><td>FWD</td><td>1</td><td>128.4115</td><td>(vpc) P2p</td></tr><tr><td>Et30</td><td>Root</td><td>FWD</td><td>1</td><td>128.4125</td><td>(vpc) P2p</td></tr></tbody></table> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 5.x (2010), at L59-60.</p>	Interface	Role	Sts	Cost	Prio.Nbr	Type	Et10	Root	FWD	2	128.4105	(vpc peer-link) P2p	Et20	Desig	FWD	1	128.4115	(vpc) P2p	Et30	Root	FWD	1	128.4125	(vpc) P2p	<p>Show commands (such as show spanning-tree) displays the RSTP instance as MST0 (MST instance 0).</p> <p>Example</p> <ul style="list-style-type: none">This command, while the switch is in RST mode, displays RST instance information. <pre>switch(config)#show spanning-tree</pre> <pre>MST0 Spanning tree enabled protocol rstp Root ID Priority 32768 Address 001c.730c.1867 Hello Time 2.000 sec Max Age 20 sec Forward Delay 15 sec This bridge is the root</pre> <p><---RSTP mode indicator</p> <table><thead><tr><th>Bridge ID</th><th>Priority</th><th>Sts</th><th>Cost</th><th>Prio.Nbr</th><th>Type</th></tr></thead><tbody><tr><td>Bridge ID</td><td>Priority</td><td>32768 (priority 32768 sys-id-ext 0)</td><td></td><td></td><td></td></tr><tr><td>Address</td><td></td><td>001c.730c.1867</td><td></td><td></td><td></td></tr><tr><td>Hello Time</td><td></td><td>2.000 sec Max Age 20 sec Forward Delay 15 sec</td><td></td><td></td><td></td></tr></tbody></table> <table><thead><tr><th>Interface</th><th>Role</th><th>State</th><th>Cost</th><th>Prio.Nbr</th><th>Type</th></tr></thead><tbody><tr><td>Et51</td><td>designated forwarding</td><td>2000</td><td>128.51</td><td>P2p</td><td></td></tr></tbody></table> <pre>switch(config)#</pre> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 960.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 838; Arista User Manual, v. 4.11.1 (1/11/13), at 656; Arista User Manual v. 4.10.3 (10/22/12), at 570; Arista User Manual v. 4.9.3.2 (5/3/12), at 490; Arista User Manual v. 4.8.2 (11/18/11), at 364; Arista User Manual v. 4.7.3 (7/18/11), at 238; Arista User Manual v. 4.6.0 (12/22/2010), at 268.</p>	Bridge ID	Priority	Sts	Cost	Prio.Nbr	Type	Bridge ID	Priority	32768 (priority 32768 sys-id-ext 0)				Address		001c.730c.1867				Hello Time		2.000 sec Max Age 20 sec Forward Delay 15 sec				Interface	Role	State	Cost	Prio.Nbr	Type	Et51	designated forwarding	2000	128.51	P2p	
	Interface	Role	Sts	Cost	Prio.Nbr	Type																																																								
	Et10	Root	FWD	2	128.4105	(vpc peer-link) P2p																																																								
Et20	Desig	FWD	1	128.4115	(vpc) P2p																																																									
Et30	Root	FWD	1	128.4125	(vpc) P2p																																																									
Bridge ID	Priority	Sts	Cost	Prio.Nbr	Type																																																									
Bridge ID	Priority	32768 (priority 32768 sys-id-ext 0)																																																												
Address		001c.730c.1867																																																												
Hello Time		2.000 sec Max Age 20 sec Forward Delay 15 sec																																																												
Interface	Role	State	Cost	Prio.Nbr	Type																																																									
Et51	designated forwarding	2000	128.51	P2p																																																										

Copyright Registration Information	Cisco	Arista																																																																																	
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<p>This example shows how to display STP information when you are running MST:</p> <pre>switch# show spanning-tree</pre> <pre>MST0000 Spanning tree enabled protocol mstp Root ID Priority 32768 Address 0018.bad8.fc150 Cost 0 Port 258 (Ethernet 2/2) Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec</pre> <pre>Bridge ID Priority 32768 (priority 32768 sys-id-ext 0) Address 0018.bad8.239d Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec</pre> <table><thead><tr><th>Interface</th><th>Role</th><th>Sts</th><th>Cost</th><th>Prio.Nbr</th><th>Type</th></tr></thead><tbody><tr><td>Eth2/1</td><td>Ach</td><td>BRN</td><td>20000</td><td>128.257</td><td>Network P2p BA_irc.</td></tr><tr><td>Eth2/2</td><td>ROOT</td><td>FWD</td><td>20000</td><td>128.258</td><td>edge, P2p</td></tr><tr><td>Eth3/48</td><td>Desg</td><td>FWD</td><td>20000</td><td>128.43228</td><td>P2p</td></tr></tbody></table> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2013), at 64</p>	Interface	Role	Sts	Cost	Prio.Nbr	Type	Eth2/1	Ach	BRN	20000	128.257	Network P2p BA_irc.	Eth2/2	ROOT	FWD	20000	128.258	edge, P2p	Eth3/48	Desg	FWD	20000	128.43228	P2p	<p>This command displays output from the show spanning-tree command:</p> <pre>Switch#show spanning-tree</pre> <pre>MST0 Spanning tree enabled protocol mstp Root ID Priority 32768 Address 0011.2201.0301 This bridge is the root</pre> <table><thead><tr><th>Bridge ID</th><th>Priority</th><th>32768 (priority 32768 sys-id-ext 0)</th></tr></thead><tbody><tr><td>Address</td><td>0011.2201.0301</td><td></td></tr><tr><td>Hello Time</td><td>2 sec</td><td>Max Age 20 sec Forward Delay 15 sec</td></tr></tbody></table> <table><thead><tr><th>Interface</th><th>Role</th><th>State</th><th>Cost</th><th>Prio.Nbr</th><th>Type</th></tr></thead><tbody><tr><td>Eth4</td><td>designated</td><td>forwarding</td><td>2000</td><td>128.4</td><td>P2p</td></tr><tr><td>Eth5</td><td>designated</td><td>forwarding</td><td>2000</td><td>128.5</td><td>P2p</td></tr><tr><td>...</td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>PEt4</td><td>designated</td><td>forwarding</td><td>2000</td><td>128.31</td><td>P2p</td></tr><tr><td>PEt5</td><td>designated</td><td>forwarding</td><td>2000</td><td>128.44</td><td>P2p</td></tr><tr><td>...</td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>Po3</td><td>designated</td><td>forwarding</td><td>1999</td><td>128.1003</td><td>P2p</td></tr></tbody></table> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 983.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 861; Arista User Manual, v. 4.11.1 (1/11/13), at 679; Arista User Manual v. 4.10.3 (10/22/12), at 593; Arista User Manual v. 4.9.3.2 (5/3/12), at 512; Arista User Manual v. 4.8.2 (11/18/11), at 386; Arista User Manual v. 4.7.3 (7/18/11), at 275; Arista User Manual v. 4.6.0 (12/22/2010), at 295</p>	Bridge ID	Priority	32768 (priority 32768 sys-id-ext 0)	Address	0011.2201.0301		Hello Time	2 sec	Max Age 20 sec Forward Delay 15 sec	Interface	Role	State	Cost	Prio.Nbr	Type	Eth4	designated	forwarding	2000	128.4	P2p	Eth5	designated	forwarding	2000	128.5	P2p	...						PEt4	designated	forwarding	2000	128.31	P2p	PEt5	designated	forwarding	2000	128.44	P2p	...						Po3	designated	forwarding	1999	128.1003	P2p
	Interface	Role	Sts	Cost	Prio.Nbr	Type																																																																													
	Eth2/1	Ach	BRN	20000	128.257	Network P2p BA_irc.																																																																													
Eth2/2	ROOT	FWD	20000	128.258	edge, P2p																																																																														
Eth3/48	Desg	FWD	20000	128.43228	P2p																																																																														
Bridge ID	Priority	32768 (priority 32768 sys-id-ext 0)																																																																																	
Address	0011.2201.0301																																																																																		
Hello Time	2 sec	Max Age 20 sec Forward Delay 15 sec																																																																																	
Interface	Role	State	Cost	Prio.Nbr	Type																																																																														
Eth4	designated	forwarding	2000	128.4	P2p																																																																														
Eth5	designated	forwarding	2000	128.5	P2p																																																																														
...																																																																																			
PEt4	designated	forwarding	2000	128.31	P2p																																																																														
PEt5	designated	forwarding	2000	128.44	P2p																																																																														
...																																																																																			
Po3	designated	forwarding	1999	128.1003	P2p																																																																														

Copyright Registration Information	Cisco	Arista																																																																																	
Cisco NX-OS 5.0 Effective date of registration: 11/13/2014	<p>This example shows how to display STP information when you are running MST:</p> <pre>switch# show spanning-tree</pre> <pre>MST0000 Spanning tree enabled protocol mstp Root ID Priority 32768 Address 0018.bad8.fc150 Cost 0 Port 258 (Ethernet 2/2) Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec</pre> <pre>Bridge ID Priority 32768 (priority 32768 sys-id-ext 0) Address 0018.bad8.239d Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec</pre> <table><thead><tr><th>Interface</th><th>Role</th><th>Sts</th><th>Cost</th><th>Prio.Nbr</th><th>Type</th></tr></thead><tbody><tr><td>Eth2/1</td><td>Alth</td><td>BRN</td><td>20000</td><td>128.257</td><td>Network P2p BA_1nc.</td></tr><tr><td>Eth2/2</td><td>ROOT</td><td>FWD</td><td>20000</td><td>128.258</td><td>edge, P2p</td></tr><tr><td>Eth3/48</td><td>Desg</td><td>FWD</td><td>20000</td><td>128.43228</td><td>P2p</td></tr></tbody></table> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 5.x (2010), at L2-59:L2-61</p>	Interface	Role	Sts	Cost	Prio.Nbr	Type	Eth2/1	Alth	BRN	20000	128.257	Network P2p BA_1nc.	Eth2/2	ROOT	FWD	20000	128.258	edge, P2p	Eth3/48	Desg	FWD	20000	128.43228	P2p	<p>This command displays output from the show spanning-tree command:</p> <pre>Switch#show spanning-tree</pre> <pre>MST0 Spanning tree enabled protocol mstp Root ID Priority 32768 Address 0011.2201.0301 This bridge is the root</pre> <table><thead><tr><th>Bridge ID</th><th>Priority</th><th>32768 (priority 32768 sys-id-ext 0)</th></tr><tr><td>Address</td><td>0011.2201.0301</td><td></td></tr><tr><td>Hello Time</td><td>2 sec</td><td>Max Age 20 sec Forward Delay 15 sec</td></tr></thead></table> <table><thead><tr><th>Interface</th><th>Role</th><th>State</th><th>Cost</th><th>Prio.Nbr</th><th>Type</th></tr></thead><tbody><tr><td>Eth4</td><td>designated</td><td>forwarding</td><td>2000</td><td>128.4</td><td>P2p</td></tr><tr><td>Eth5</td><td>designated</td><td>forwarding</td><td>2000</td><td>128.5</td><td>P2p</td></tr><tr><td>...</td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>PEt4</td><td>designated</td><td>forwarding</td><td>2000</td><td>128.31</td><td>P2p</td></tr><tr><td>PEt5</td><td>designated</td><td>forwarding</td><td>2000</td><td>128.44</td><td>P2p</td></tr><tr><td>...</td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>Po3</td><td>designated</td><td>forwarding</td><td>1999</td><td>128.1003</td><td>P2p</td></tr></tbody></table> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 983.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 861; Arista User Manual, v. 4.11.1 (1/11/13), at 679; Arista User Manual v. 4.10.3 (10/22/12), at 593; Arista User Manual v. 4.9.3.2 (5/3/12), at 512; Arista User Manual v. 4.8.2 (11/18/11), at 386; Arista User Manual v. 4.7.3 (7/18/11), at 275; Arista User Manual v. 4.6.0 (12/22/2010), at 295</p>	Bridge ID	Priority	32768 (priority 32768 sys-id-ext 0)	Address	0011.2201.0301		Hello Time	2 sec	Max Age 20 sec Forward Delay 15 sec	Interface	Role	State	Cost	Prio.Nbr	Type	Eth4	designated	forwarding	2000	128.4	P2p	Eth5	designated	forwarding	2000	128.5	P2p	...						PEt4	designated	forwarding	2000	128.31	P2p	PEt5	designated	forwarding	2000	128.44	P2p	...						Po3	designated	forwarding	1999	128.1003	P2p
	Interface	Role	Sts	Cost	Prio.Nbr	Type																																																																													
Eth2/1	Alth	BRN	20000	128.257	Network P2p BA_1nc.																																																																														
Eth2/2	ROOT	FWD	20000	128.258	edge, P2p																																																																														
Eth3/48	Desg	FWD	20000	128.43228	P2p																																																																														
Bridge ID	Priority	32768 (priority 32768 sys-id-ext 0)																																																																																	
Address	0011.2201.0301																																																																																		
Hello Time	2 sec	Max Age 20 sec Forward Delay 15 sec																																																																																	
Interface	Role	State	Cost	Prio.Nbr	Type																																																																														
Eth4	designated	forwarding	2000	128.4	P2p																																																																														
Eth5	designated	forwarding	2000	128.5	P2p																																																																														
...																																																																																			
PEt4	designated	forwarding	2000	128.31	P2p																																																																														
PEt5	designated	forwarding	2000	128.44	P2p																																																																														
...																																																																																			
Po3	designated	forwarding	1999	128.1003	P2p																																																																														

Copyright Registration Information	Cisco	Arista																																																												
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<div>Spanning tree enabled protocol rstp</div> <div><div>Root ID</div><div>Priority</div><div>32768</div></div> <div><div>Address</div><div>000d.eca3.9f01</div></div> <div><div>Cost</div><div>4</div></div> <div><div>Port</div><div>4105 (port-channel10)</div></div> <div><div>Hello Time</div><div>2 sec</div><div>Max Age 20 sec</div><div>Forward Delay 15 sec</div></div> <div><div>Bridge ID</div><div>Priority</div><div>32770 (priority 32768 sys-id-ext 2)</div></div> <div><div>Address</div><div>0022.5579.7641</div></div> <div><div>Hello Time</div><div>2 sec</div><div>Max Age 20 sec</div><div>Forward Delay 15 sec</div></div> <div><table><thead><tr><th>Interface</th><th>Role</th><th>Sts</th><th>Cost</th><th>Prio.Nbr</th><th>Type</th></tr></thead><tbody><tr><td>Po10</td><td>Root</td><td>FWD</td><td>2</td><td>128.4105</td><td>(vPC peer-link) P2p</td></tr><tr><td>Po20</td><td>Desg</td><td>FWD</td><td>1</td><td>128.4115</td><td>(vPC) P2p</td></tr><tr><td>Po30</td><td>Root</td><td>FWD</td><td>1</td><td>128.4125</td><td>(vPC) P2p</td></tr></tbody></table></div> <div>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference at 67</div>	Interface	Role	Sts	Cost	Prio.Nbr	Type	Po10	Root	FWD	2	128.4105	(vPC peer-link) P2p	Po20	Desg	FWD	1	128.4115	(vPC) P2p	Po30	Root	FWD	1	128.4125	(vPC) P2p	<div>Spanning tree enabled protocol rstp</div> <div><div>Root ID</div><div>Priority</div><div>32768</div></div> <div><div>Address</div><div>001c.7301.07b9</div></div> <div><div>Cost</div><div>1999 (Ext) 0 (Int)</div></div> <div><div>Port</div><div>101 (Port-Channel12)</div></div> <div><div>Hello Time</div><div>2.000 sec</div><div>Max Age 20 sec</div><div>Forward Delay 15 sec</div></div> <div><div>Bridge ID</div><div>Priority</div><div>32768 (priority 32768 sys-id-ext 0)</div></div> <div><div>Address</div><div>001c.7304.195b</div></div> <div><div>Hello Time</div><div>2.000 sec</div><div>Max Age 20 sec</div><div>Forward Delay 15 sec</div></div> <div><table><thead><tr><th>Interface</th><th>Role</th><th>State</th><th>Cost</th><th>Prio.Nbr</th><th>Type</th></tr></thead><tbody><tr><td>Et4</td><td>designated forwarding</td><td>20000</td><td>128.4</td><td>P2p</td></tr><tr><td>Et5</td><td>designated forwarding</td><td>20000</td><td>128.5</td><td>P2p</td></tr><tr><td>Et6</td><td>designated forwarding</td><td>20000</td><td>128.6</td><td>P2p</td></tr><tr><td>Et23</td><td>designated forwarding</td><td>20000</td><td>128.23</td><td>P2p</td></tr><tr><td>Et26</td><td>designated forwarding</td><td>20000</td><td>128.26</td><td>P2p</td></tr><tr><td>Et32</td><td>designated forwarding</td><td>2000</td><td>128.32</td><td>P2p</td></tr></tbody></table></div> <div>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 983.</div> <div>See also Arista User Manual v. 4.12.3 (7/17/13), at 861; Arista User Manual, v. 4.11.1 (1/11/13), at 679; Arista User Manual v. 4.10.3 (10/22/12), at 593; Arista User Manual v. 4.9.3.2 (5/3/12), at 512; Arista User Manual v. 4.8.2 (11/18/11), at 386; Arista User Manual v. 4.7.3 (7/18/11), at 275; Arista User Manual v. 4.6.0 (12/22/2010), at 268</div>	Interface	Role	State	Cost	Prio.Nbr	Type	Et4	designated forwarding	20000	128.4	P2p	Et5	designated forwarding	20000	128.5	P2p	Et6	designated forwarding	20000	128.6	P2p	Et23	designated forwarding	20000	128.23	P2p	Et26	designated forwarding	20000	128.26	P2p	Et32	designated forwarding	2000	128.32	P2p
	Interface	Role	Sts	Cost	Prio.Nbr	Type																																																								
	Po10	Root	FWD	2	128.4105	(vPC peer-link) P2p																																																								
Po20	Desg	FWD	1	128.4115	(vPC) P2p																																																									
Po30	Root	FWD	1	128.4125	(vPC) P2p																																																									
Interface	Role	State	Cost	Prio.Nbr	Type																																																									
Et4	designated forwarding	20000	128.4	P2p																																																										
Et5	designated forwarding	20000	128.5	P2p																																																										
Et6	designated forwarding	20000	128.6	P2p																																																										
Et23	designated forwarding	20000	128.23	P2p																																																										
Et26	designated forwarding	20000	128.26	P2p																																																										
Et32	designated forwarding	2000	128.32	P2p																																																										

Copyright Registration Information	Cisco	Arista																																																																		
Cisco NX-OS 5.0 Effective date of registration: 11/13/2014	<div>Spanning tree enabled protocol rstp</div> <div><div>Root ID</div><div>Priority</div><div>32768</div></div> <div><div>Address</div><div>000d.eca3.9f01</div></div> <div><div>Cost</div><div>4</div></div> <div><div>Port</div><div>4105 (port-channel10)</div></div> <div><div>Hello Time</div><div>2 sec</div><div>Max Age 20 sec</div><div>Forward Delay 15 sec</div></div> <div><div>Bridge ID</div><div>Priority</div><div>32770 (priority 32768 sys-id-ext 2)</div></div> <div><div>Address</div><div>0022.5579.7641</div></div> <div><div>Hello Time</div><div>2 sec</div><div>Max Age 20 sec</div><div>Forward Delay 15 sec</div></div> <div><table><thead><tr><th>Interface</th><th>Role</th><th>Sts</th><th>Cost</th><th>Prio.Nbr</th><th>Type</th></tr></thead><tbody><tr><td>Po10</td><td>Root</td><td>FWD</td><td>2</td><td>128.4105</td><td>(vPC peer-link) P2p</td></tr><tr><td>Po20</td><td>Desg</td><td>FWD</td><td>1</td><td>128.4115</td><td>(vPC) P2p</td></tr><tr><td>Po30</td><td>Root</td><td>FWD</td><td>1</td><td>128.4125</td><td>(vPC) P2p</td></tr></tbody></table></div> <div>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 5.x (2010), at L2-59:L2-64</div>	Interface	Role	Sts	Cost	Prio.Nbr	Type	Po10	Root	FWD	2	128.4105	(vPC peer-link) P2p	Po20	Desg	FWD	1	128.4115	(vPC) P2p	Po30	Root	FWD	1	128.4125	(vPC) P2p	<div>Spanning tree enabled protocol rstp</div> <div><div>Root ID</div><div>Priority</div><div>32768</div></div> <div><div>Address</div><div>001c.7301.07b9</div></div> <div><div>Cost</div><div>1999 (Ext) 0 (Int)</div></div> <div><div>Port</div><div>101 (Port-Channel12)</div></div> <div><div>Hello Time</div><div>2.000 sec</div><div>Max Age 20 sec</div><div>Forward Delay 15 sec</div></div> <div><div>Bridge ID</div><div>Priority</div><div>32768 (priority 32768 sys-id-ext 0)</div></div> <div><div>Address</div><div>001c.7304.195b</div></div> <div><div>Hello Time</div><div>2.000 sec</div><div>Max Age 20 sec</div><div>Forward Delay 15 sec</div></div> <div><table><thead><tr><th>Interface</th><th>Role</th><th>State</th><th>Cost</th><th>Prio.Nbr</th><th>Type</th></tr></thead><tbody><tr><td>Et4</td><td>designated forwarding</td><td></td><td>20000</td><td>128.4</td><td>P2p</td></tr><tr><td>Et5</td><td>designated forwarding</td><td></td><td>20000</td><td>128.5</td><td>P2p</td></tr><tr><td>Et6</td><td>designated forwarding</td><td></td><td>20000</td><td>128.6</td><td>P2p</td></tr><tr><td>Et23</td><td>designated forwarding</td><td></td><td>20000</td><td>128.23</td><td>P2p</td></tr><tr><td>Et26</td><td>designated forwarding</td><td></td><td>20000</td><td>128.26</td><td>P2p</td></tr><tr><td>Et32</td><td>designated forwarding</td><td></td><td>2000</td><td>128.32</td><td>P2p</td></tr></tbody></table></div> <div>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 983.</div> <div>See also Arista User Manual v. 4.12.3 (7/17/13), at 861; Arista User Manual, v. 4.11.1 (1/11/13), at 679; Arista User Manual v. 4.10.3 (10/22/12), at 593; Arista User Manual v. 4.9.3.2 (5/3/12), at 512; Arista User Manual v. 4.8.2 (11/18/11), at 386; Arista User Manual v. 4.7.3 (7/18/11), at 275; Arista User Manual v. 4.6.0 (12/22/2010), at 268</div>	Interface	Role	State	Cost	Prio.Nbr	Type	Et4	designated forwarding		20000	128.4	P2p	Et5	designated forwarding		20000	128.5	P2p	Et6	designated forwarding		20000	128.6	P2p	Et23	designated forwarding		20000	128.23	P2p	Et26	designated forwarding		20000	128.26	P2p	Et32	designated forwarding		2000	128.32	P2p
	Interface	Role	Sts	Cost	Prio.Nbr	Type																																																														
	Po10	Root	FWD	2	128.4105	(vPC peer-link) P2p																																																														
Po20	Desg	FWD	1	128.4115	(vPC) P2p																																																															
Po30	Root	FWD	1	128.4125	(vPC) P2p																																																															
Interface	Role	State	Cost	Prio.Nbr	Type																																																															
Et4	designated forwarding		20000	128.4	P2p																																																															
Et5	designated forwarding		20000	128.5	P2p																																																															
Et6	designated forwarding		20000	128.6	P2p																																																															
Et23	designated forwarding		20000	128.23	P2p																																																															
Et26	designated forwarding		20000	128.26	P2p																																																															
Et32	designated forwarding		2000	128.32	P2p																																																															

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>This example shows how to display detailed information about the STP configuration:</p> <pre>switch(config)# show spanning-tree detail</pre> <p>VLAN0001 is executing the rstp compatible Spanning Tree protocol</p> <p>Bridge Identifier has priority 32768, sysid 1, address 0022.5579.7641</p> <p>Configured hello time 2, max age 20, forward delay 15</p> <p>Current root has priority 32769, address 000d.eca3.9f01</p> <p>Root port is 4105 (port-channel10), cost of root path is 4</p> <p>Topology change flag not set, detected flag not set</p> <p>Number of topology changes 1 last change occurred 20:24:36 ago</p> <p>from port-channel10</p> <p>Timers: hold 1, topology change 35, notification 2</p> <p>hello 2, max age 20, forward delay 15</p> <p>Timers: hello 0, topology change 0, notification 0</p> <p>Port 4105 (port-channel10, VPC Peer-link) of VLAN0001 is root forwarding</p> <p>Port path cost 2, Port priority 128, Port Identifier 128.4105</p> <p>Designated root has priority 32769, address 000d.eca3.9f01</p> <p>Designated bridge has priority 32769, address 0022.5579.7341</p> <p>Designated port id is 128.4105, designated path cost 2</p> <p>Timers: message age 16, forward delay 0, hold 0</p> <p>Number of transitions to forwarding state: 1</p> <p>Link type is point-to-point by default</p> <p>BPDU: sent 36729, received 36739</p> <p>Port 4115 (port-channel20, VPC) of VLAN0001 is designated forwarding</p> <p>Port path cost 1, Port priority 128, Port Identifier 128.4115</p> <p>Designated root has priority 32769, address 000d.eca3.9f01</p> <p>Designated bridge has priority 32769, address 0022.5579.7341</p> <p>Designated port id is 128.4115, designated path cost 2</p> <p>Timers: message age 0, forward delay 0, hold 0</p> <p>Number of transitions to forwarding state: 0</p> <p>Link type is point-to-point by default</p> <p>BPDU: sent 0, received 0</p> <p>Port 4125 (port-channel30, VPC) of VLAN0001 is root forwarding</p> <p>Port path cost 1, Port priority 128, Port Identifier 128.4125</p> <p>Designated root has priority 32769, address 000d.eca3.9f01</p> <p>Designated bridge has priority 32769, address 000d.eca3.9f01</p> <p>Designated port id is 128.4125, designated path cost 0</p> <p>Timers: message age 0, forward delay 0, hold 0</p> <p>Number of transitions to forwarding state: 0</p> <p>Link type is point-to-point by default</p> <p>BPDU: sent 0, received 0</p> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2013), at 74-75 Release 6.x (2013), at 73</p>	<p>• This command displays STP data, including an information block for each interface running STP.</p> <pre>switch>show spanning-tree vlan 1000 detail</pre> <p>MST0 is executing the rstp Spanning Tree protocol</p> <p>Bridge Identifier has priority 32768, sysid 0, address 001c.7304.195b</p> <p>Configured hello time 2.000, max age 20, forward delay 15, transmit hold-count 6</p> <p>Current root has priority 32768, address 001c.7301.07b9</p> <p>Root port is 101 (Port-Channel2), cost of root path is 1999 (Ext) 0 (Int)</p> <p>Number of topology changes 4109 last change occurred 1292651 seconds ago</p> <p>from Ethernet13</p> <p>Port 4 (Ethernet4) of MST0 is designated forwarding</p> <p>Port path cost 20000, Port priority 128, Port Identifier 128.4.</p> <p>Designated root has priority 32768, address 001c.7301.07b9</p> <p>Designated bridge has priority 32768, address 001c.7304.195b</p> <p>Designated port id is 128.4, designated path cost 1999 (Ext) 0 (Int)</p> <p>Timers: message age 1, forward delay 15, hold 20</p> <p>Number of transitions to forwarding state: 1</p> <p>Link type is point-to-point by default, Internal</p> <p>BPDU: sent 452252, received 0, taggedErr 0, otherErr 0, rateLimiterCount 0</p> <p>Rate-Limiter: enabled, Window: 10 sec, Max-BPDU: 400</p> <p>Port 5 (Ethernet5) of MST0 is designated forwarding</p> <p>Port path cost 20000, Port priority 128, Port Identifier 128.5.</p> <p>Designated root has priority 32768, address 001c.7301.07b9</p> <p>Designated bridge has priority 32768, address 001c.7304.195b</p> <p>Designated port id is 128.5, designated path cost 1999 (Ext) 0 (Int)</p> <p>Timers: message age 1, forward delay 15, hold 20</p> <p>Number of transitions to forwarding state: 1</p> <p>Link type is point-to-point by default, Internal</p> <p>BPDU: sent 1006266, received 0, taggedErr 0, otherErr 0, rateLimiterCount 0</p> <p>Rate-Limiter: enabled, Window: 10 sec, Max-BPDU: 400</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 984.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 862; Arista User Manual, v. 4.11.1 (1/11/13), at 680; Arista User Manual v. 4.10.3 (10/22/12), at 594; Arista User Manual v. 4.9.3.2 (5/3/12), at 513; Arista User Manual v. 4.8.2 (11/18/11), at 387; Arista User Manual v. 4.7.3 (7/18/11), at 276.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 5.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>This example shows how to display detailed information about the STP configuration:</p> <pre>switch(config)# show spanning-tree detail</pre> <p>VLAN0001 is executing the rstp compatible Spanning Tree protocol</p> <p>Bridge Identifier has priority 32768, sysid 1, address 0022.5579.7641</p> <p>Configured hello time 2, max age 20, forward delay 15</p> <p>Current root has priority 32769, address 000d.eca3.9f01</p> <p>Root port is 4105 (port-channel10), cost of root path is 4</p> <p>Topology change flag not set, detected flag not set</p> <p>Number of topology changes 1 last change occurred 20:24:36 ago</p> <p>from port-channel10</p> <p>Timers: hold 1, topology change 35, notification 2</p> <p>hello 2, max age 20, forward delay 15</p> <p>Timers: hello 0, topology change 0, notification 0</p> <p>Port 4105 (port-channel10, VPC Peer-link) of VLAN0001 is root forwarding</p> <p>Port path cost 2, Port priority 128, Port Identifier 128.4105</p> <p>Designated root has priority 32769, address 000d.eca3.9f01</p> <p>Designated bridge has priority 32769, address 0022.5579.7341</p> <p>Designated port id is 128.4105, designated path cost 2</p> <p>Timers: message age 16, forward delay 0, hold 0</p> <p>Number of transitions to forwarding state: 1</p> <p>Link type is point-to-point by default</p> <p>BPDU: sent 36729, received 36739</p> <p>Port 4115 (port-channel20, VPC) of VLAN0001 is designated forwarding</p> <p>Port path cost 1, Port priority 128, Port Identifier 128.4115</p> <p>Designated root has priority 32769, address 000d.eca3.9f01</p> <p>Designated bridge has priority 32769, address 0022.5579.7341</p> <p>Designated port id is 128.4115, designated path cost 2</p> <p>Timers: message age 0, forward delay 0, hold 0</p> <p>Number of transitions to forwarding state: 0</p> <p>Link type is point-to-point by default</p> <p>BPDU: sent 0, received 0</p> <p>Port 4125 (port-channel30, VPC) of VLAN0001 is root forwarding</p> <p>Port path cost 1, Port priority 128, Port Identifier 128.4125</p> <p>Designated root has priority 32769, address 000d.eca3.9f01</p> <p>Designated bridge has priority 32769, address 000d.eca3.9f01</p> <p>Designated port id is 128.4125, designated path cost 0</p> <p>Timers: message age 0, forward delay 0, hold 0</p> <p>Number of transitions to forwarding state: 0</p> <p>Link type is point-to-point by default</p> <p>BPDU: sent 0, received 0</p> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2010), at L2-71:L2-72</p>	<ul style="list-style-type: none"> This command displays STP data, including an information block for each interface running STP. <pre>switch>show spanning-tree vlan 1000 detail</pre> <p>MST0 is executing the rstp Spanning Tree protocol</p> <p>Bridge Identifier has priority 32768, sysid 0, address 001c.7304.195b</p> <p>Configured hello time 2.000, max age 20, forward delay 15, transmit hold-count 6</p> <p>Current root has priority 32768, address 001c.7301.07b9</p> <p>Root port is 101 (Port-Channel2), cost of root path is 1999 (Ext) 0 (Int)</p> <p>Number of topology changes 4109 last change occurred 1292651 seconds ago</p> <p>from Ethernet13</p> <p>Port 4 (Ethernet4) of MST0 is designated forwarding</p> <p>Port path cost 20000, Port priority 128, Port Identifier 128.4.</p> <p>Designated root has priority 32768, address 001c.7301.07b9</p> <p>Designated bridge has priority 32768, address 001c.7304.195b</p> <p>Designated port id is 128.4, designated path cost 1999 (Ext) 0 (Int)</p> <p>Timers: message age 1, forward delay 15, hold 20</p> <p>Number of transitions to forwarding state: 1</p> <p>Link type is point-to-point by default, Internal</p> <p>BPDU: sent 452252, received 0, taggedErr 0, otherErr 0, rateLimiterCount 0</p> <p>Rate-Limiter: enabled, Window: 10 sec, Max-BPDU: 400</p> <p>Port 5 (Ethernet5) of MST0 is designated forwarding</p> <p>Port path cost 20000, Port priority 128, Port Identifier 128.5.</p> <p>Designated root has priority 32768, address 001c.7301.07b9</p> <p>Designated bridge has priority 32768, address 001c.7304.195b</p> <p>Designated port id is 128.5, designated path cost 1999 (Ext) 0 (Int)</p> <p>Timers: message age 1, forward delay 15, hold 20</p> <p>Number of transitions to forwarding state: 1</p> <p>Link type is point-to-point by default, Internal</p> <p>BPDU: sent 1006266, received 0, taggedErr 0, otherErr 0, rateLimiterCount 0</p> <p>Rate-Limiter: enabled, Window: 10 sec, Max-BPDU: 400</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 984.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 862; Arista User Manual, v. 4.11.1 (1/11/13), at 680; Arista User Manual v. 4.10.3 (10/22/12), at 594; Arista User Manual v. 4.9.3.2 (5/3/12), at 513; Arista User Manual v. 4.8.2 (11/18/11), at 387; Arista User Manual v. 4.7.3 (7/18/11), at 276.</p>

Copyright Registration Information	Cisco	Arista																																												
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<p>This example shows how to display STP information about a specified interface when you are running Rapid PVST+:</p> <pre>switch(config)# show spanning-tree interface ethernet 8/2</pre> <table><thead><tr><th>Vlan</th><th>Role</th><th>Sts</th><th>Cost</th><th>Prio.Nbr</th><th>Type</th></tr></thead><tbody><tr><td>VLAN0001</td><td>Altn</td><td>BLK</td><td>20000</td><td>128.1025</td><td>P2p</td></tr><tr><td>VLAN0002</td><td>Desg</td><td>FWD</td><td>20000</td><td>128.1025</td><td>P2p</td></tr></tbody></table> <p>This example shows how to display STP information about a specified interface when you are running MST:</p> <pre>switch(config)# show spanning-tree interface ethernet 2/50</pre> <table><thead><tr><th>Mst</th><th>Instance</th><th>Role</th><th>Sts</th><th>Cost</th><th>Prio.Nbr</th><th>Type</th></tr></thead><tbody><tr><td>MST0000</td><td></td><td>Desg</td><td>FWD</td><td>20000</td><td>128.1281</td><td>P2p</td></tr></tbody></table> <p>This example shows how to display detailed STP information about a specified interface when you are running Rapid PVST+:</p> <pre>switch(config)# show spanning-tree interface ethernet 8/1 detail</pre> <p>Port 1025 (Ethernet8/1) of VLAN0001 is alternate blocking Port path cost 20000, Port priority 128, Port Identifier 128.1025 Designated root has priority 28672, address 0018.bad8.239d Designated bridge has priority 28672, address 0018.bad8.239d Designated port id is 128.1281, designated path cost 0 Timers: message age 15, forward delay 0, hold 0 Number of transitions to forwarding state: 1 Link type is point-to-point by default The port type is network by default. BPDUs: sent 4657, received 188</p> <p>Port 1025 (Ethernet8/1) of VLAN0002 is designated forwarding Port path cost 20000, Port priority 128, Port Identifier 128.1025 Designated root has priority 32770, address 0018.bad7.fc15 Designated bridge has priority 32770, address 0018.bad7.fc15 Designated port id is 128.1025, designated path cost 0 Timers: message age 0, forward delay 0, hold 0 Number of transitions to forwarding state: 1 Link type is point-to-point by default The port type is network by default. BPDUs: sent 4838, received 0</p>	Vlan	Role	Sts	Cost	Prio.Nbr	Type	VLAN0001	Altn	BLK	20000	128.1025	P2p	VLAN0002	Desg	FWD	20000	128.1025	P2p	Mst	Instance	Role	Sts	Cost	Prio.Nbr	Type	MST0000		Desg	FWD	20000	128.1281	P2p	<p>Examples</p> <ul style="list-style-type: none">This command displays an STP table for Ethernet 5 interface. <pre>switch# show spanning-tree interface ethernet 5</pre> <table><thead><tr><th>Instance</th><th>Role</th><th>State</th><th>Cost</th><th>Prio.Nbr</th><th>Type</th></tr></thead><tbody><tr><td>MST0</td><td>designated</td><td>forwarding</td><td>20000</td><td>128.5</td><td>P2p</td></tr></tbody></table> <pre>switch></pre> <ul style="list-style-type: none">This command displays a data block for Ethernet interface 5. <pre>switch# show spanning-tree interface ethernet 5 detail</pre> <p>Port 5 (Ethernet5) of MST0 is designated forwarding Port path cost 20000, Port priority 128, Port Identifier 128.5. Designated root has priority 32768, address 001c.7301.07b9 Designated bridge has priority 32768, address 001c.7304.195b Designated port id is 128.5, designated path cost 1999 (Ext) 0 (Int) Timers: message age 1, forward delay 15, hold 20 Number of transitions to forwarding state: 1 Link type is point-to-point by default, Internal BPDUs: sent 1008766, received 0, taggedErr 0, otherErr 0, rateLimiterCount 0 Rate-Limiter: enabled, Window: 10 sec, Max-BPDU: 400</p> <pre>switch></pre>	Instance	Role	State	Cost	Prio.Nbr	Type	MST0	designated	forwarding	20000	128.5	P2p
	Vlan	Role	Sts	Cost	Prio.Nbr	Type																																								
	VLAN0001	Altn	BLK	20000	128.1025	P2p																																								
VLAN0002	Desg	FWD	20000	128.1025	P2p																																									
Mst	Instance	Role	Sts	Cost	Prio.Nbr	Type																																								
MST0000		Desg	FWD	20000	128.1281	P2p																																								
Instance	Role	State	Cost	Prio.Nbr	Type																																									
MST0	designated	forwarding	20000	128.5	P2p																																									
		<p>Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 988.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 866; Arista User Manual, v. 4.11.1 (1/11/13), at 684; Arista User Manual v. 4.10.3 (10/22/12), at 598; Arista User Manual v. 4.9.3.2 (5/3/12), at 517; Arista User Manual v. 4.8.2 (11/18/11), at 391; Arista User Manual v. 4.7.3 (7/18/11), at 280.</p>																																												
	Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2013), at 77.																																													

Copyright Registration Information	Cisco	Arista																																												
Cisco NX-OS 5.0 Effective date of registration: 11/13/2014	<p>This example shows how to display STP information about a specified interface when you are running Rapid PVST+:</p> <pre>switch(config)# show spanning-tree interface ethernet 8/2</pre> <table><thead><tr><th>Vlan</th><th>Role</th><th>Sts</th><th>Cost</th><th>Prio.Nbr</th><th>Type</th></tr></thead><tbody><tr><td>VLAN0001</td><td>Altn</td><td>BLK</td><td>20000</td><td>128.1025</td><td>P2p</td></tr><tr><td>VLAN0002</td><td>Desg</td><td>FWD</td><td>20000</td><td>128.1025</td><td>P2p</td></tr></tbody></table> <p>This example shows how to display STP information about a specified interface when you are running MST:</p> <pre>switch(config)# show spanning-tree interface ethernet 2/50</pre> <table><thead><tr><th>Mst</th><th>Instance</th><th>Role</th><th>Sts</th><th>Cost</th><th>Prio.Nbr</th><th>Type</th></tr></thead><tbody><tr><td>MST0000</td><td></td><td>Desg</td><td>FWD</td><td>20000</td><td>128.1281</td><td>P2p</td></tr></tbody></table> <p>This example shows how to display detailed STP information about a specified interface when you are running Rapid PVST+:</p> <pre>switch(config)# show spanning-tree interface ethernet 8/1 detail</pre> <p>Port 1025 (Ethernet8/1) of VLAN0001 is alternate blocking Port path cost 20000, Port priority 128, Port Identifier 128.1025 Designated root has priority 28672, address 0018.bad8.239d Designated bridge has priority 28672, address 0018.bad8.239d Designated port id is 128.1281, designated path cost 0 Timers: message age 15, forward delay 0, hold 0 Number of transitions to forwarding state: 1 Link type is point-to-point by default The port type is network by default. BPDUs: sent 4657, received 188</p> <p>Port 1025 (Ethernet8/1) of VLAN0002 is designated forwarding Port path cost 20000, Port priority 128, Port Identifier 128.1025 Designated root has priority 32770, address 0018.bad7.fc15 Designated bridge has priority 32770, address 0018.bad7.fc15 Designated port id is 128.1025, designated path cost 0 Timers: message age 0, forward delay 0, hold 0 Number of transitions to forwarding state: 1 Link type is point-to-point by default The port type is network by default. BPDUs: sent 4838, received 0</p>	Vlan	Role	Sts	Cost	Prio.Nbr	Type	VLAN0001	Altn	BLK	20000	128.1025	P2p	VLAN0002	Desg	FWD	20000	128.1025	P2p	Mst	Instance	Role	Sts	Cost	Prio.Nbr	Type	MST0000		Desg	FWD	20000	128.1281	P2p	<p>Examples</p> <ul style="list-style-type: none">This command displays an STP table for Ethernet 5 interface. <pre>switch# show spanning-tree interface ethernet 5</pre> <table><thead><tr><th>Instance</th><th>Role</th><th>State</th><th>Cost</th><th>Prio.Nbr</th><th>Type</th></tr></thead><tbody><tr><td>MST0</td><td>designated</td><td>forwarding</td><td>20000</td><td>128.5</td><td>P2p</td></tr></tbody></table> <p>switch></p> <ul style="list-style-type: none">This command displays a data block for Ethernet interface 5. <pre>switch# show spanning-tree interface ethernet 5 detail</pre> <p>Port 5 (Ethernet5) of MST0 is designated forwarding Port path cost 20000, Port priority 128, Port Identifier 128.5. Designated root has priority 32768, address 001c.7301.07b9 Designated bridge has priority 32768, address 001c.7304.195b Designated port id is 128.5, designated path cost 1999 (Ext) 0 (Int) Timers: message age 1, forward delay 15, hold 20 Number of transitions to forwarding state: 1 Link type is point-to-point by default, Internal BPDU: sent 1008766, received 0, taggedErr 0, otherErr 0, rateLimiterCount 0 Rate-Limiter: enabled, Window: 10 sec, Max-BPDU: 400</p> <p>switch></p>	Instance	Role	State	Cost	Prio.Nbr	Type	MST0	designated	forwarding	20000	128.5	P2p
	Vlan	Role	Sts	Cost	Prio.Nbr	Type																																								
VLAN0001	Altn	BLK	20000	128.1025	P2p																																									
VLAN0002	Desg	FWD	20000	128.1025	P2p																																									
Mst	Instance	Role	Sts	Cost	Prio.Nbr	Type																																								
MST0000		Desg	FWD	20000	128.1281	P2p																																								
Instance	Role	State	Cost	Prio.Nbr	Type																																									
MST0	designated	forwarding	20000	128.5	P2p																																									
	<p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2010), at L2-74</p>	<p>Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 988.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 866; Arista User Manual, v. 4.11.1 (1/11/13), at 684; Arista User Manual v. 4.10.3 (10/22/12), at 598; Arista User Manual v. 4.9.3.2 (5/3/12), at 517; Arista User Manual v. 4.8.2 (11/18/11), at 391; Arista User Manual v. 4.7.3 (7/18/11), at 280.</p>																																												

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<pre> switch# show spanning-tree mst #### MST0 vlans mapped: 1-4094 Bridge address 0019.bad7.fc15 priority 32768 (32768 sysid 0) Root this switch for the CIST Regional Root this switch Operational hello time 2 , forward delay 15, max age 20, txholdcount 6 Configured hello time 2 , forward delay 15, max age 20, max hops 20 Interface Role Sts Cost Prio.Nbr Type ----- Eth8/1 Desg FWD 20000 128.1025 P2p Eth8/2 Desg FWD 20000 128.1026 P2p This example shows how to display STP information about a specific MST instance: switch# show spanning-tree mst 0 #### MST0 vlans mapped: 1-4094 Bridge address 0019.bad7.fc15 priority 32768 (32768 sysid 0) Root this switch for the CIST Regional Root this switch Operational hello time 2 , forward delay 15, max age 20, txholdcount 6 Configured hello time 2 , forward delay 15, max age 20, max hops 20 Interface Role State Cost Prio.Nbr Type ----- Eth8/1 Desg FWD 20000 128.1025 P2p Eth8/2 Desg FWD 20000 128.1026 P2p This example shows how to display detailed STP information about the MST protocol: switch# show spanning-tree mst detail #### MST0 vlans mapped: 1-4094 Bridge address 0019.bad7.fc15 priority 32768 (32768 sysid 0) Root this switch for the CIST Regional Root this switch Operational hello time 2 , forward delay 15, max age 20, txholdcount 6 Configured hello time 2 , forward delay 15, max age 20, max hops 20 Eth8/1 of MST0 is designated forwarding Port info port id 128.1025 priority 128 cost 20000 Designated root address 0019.bad7.fc15 priority 32768 cost 0 Design. regional root address 0019.bad7.fc15 priority 32768 cost 0 Designated bridge address 0019.bad7.fc15 priority 32768 port id 128.1025 Timers: message expires in 0 sec, forward delay 0, forward transitions 1 Bpdus sent 1379, received 3 Eth8/2 of MST0 is designated forwarding Port info port id 128.1026 priority 128 cost 20000 Designated root address 0019.bad7.fc15 priority 32768 cost 0 Design. regional root address 0019.bad7.fc15 priority 32768 cost 0 Designated bridge address 0019.bad7.fc15 priority 32768 port id 128.1026 Timers: message expires in 0 sec, forward delay 0, forward transitions 1 Bpdus sent 1380, received 2 </pre> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2013), at 80.</p>	<p>Examples</p> <ul style="list-style-type: none"> This command displays interface data blocks for MST instance 3. <pre> switch# show spanning-tree mst 3 detail #### MST3 vlans mapped: 2 Bridge address 0011.2233.4402 priority 32771 (32768 sysid 3) Root address 0011.2233.4401 priority 32771 (32768 sysid 3) Ethernet1 of MST3 is root forwarding Port info port id 128.1 priority 128 cost 2000 Designated root address 0011.2233.4401 priority 32768 cost 0 Designated bridge address 0011.2233.4401 priority 32768 port id 128.1 Ethernet2 of MST3 is alternate discarding Port info port id 128.2 priority 128 cost 2000 Designated root address 0011.2233.4401 priority 32768 cost 0 Designated bridge address 0011.2233.4401 priority 32768 port id 128.2 Ethernet3 of MST3 is designated forwarding Port info port id 128.3 priority 128 cost 2000 Designated root address 0011.2233.4401 priority 32768 cost 2000 Designated bridge address 0011.2233.4402 priority 32768 port id 128.3 </pre> <ul style="list-style-type: none"> This command displays interface tables for all MST instances. <pre> switch# show spanning-tree mst #### MST0 vlans mapped: 1-4094 Bridge address 0011.2233.4402 priority 32768 (32768 sysid 0) Root address 0011.2233.4401 priority 32768 (32768 sysid 0) Regional Root address 0011.2233.4401 priority 32768 (32768 sysid 0) Interface Role State Cost Prio.Nbr Type ----- Et1 root forwarding 2000 128.1 P2p Et2 alternate discarding 2000 128.2 P2p Et3 designated forwarding 2000 128.3 P2p Et4 designated forwarding 2000 128.4 P2p #### MST2 vlans mapped: 3 Bridge address 0011.2233.4402 priority 8194 (8192 sysid 2) Root this switch for MST2 Interface Role State Cost Prio.Nbr Type ----- Et1 designated forwarding 2000 128.1 P2p Et2 designated forwarding 2000 128.2 P2p Et3 designated forwarding 2000 128.3 P2p Et4 designated forwarding 2000 128.4 P2p #### MST3 vlans mapped: 3 Bridge address 0011.2233.4402 priority 32771 (32768 sysid 3) Root address 0011.2233.4401 priority 32771 (32768 sysid 3) Interface Role State Cost Prio.Nbr Type ----- Et1 root forwarding 2000 128.1 P2p Et2 alternate discarding 2000 128.2 P2p Et3 designated forwarding 2000 128.3 P2p Et4 designated forwarding 2000 128.4 P2p </pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 990.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 867-68; Arista User Manual, v. 4.11.1 (1/11/13), at 685-86; Arista User Manual v. 4.10.3 (10/22/12), at 599-600; Arista User Manual v. 4.9.3.2 (5/3/12), at 518-19; Arista User Manual v. 4.8.2 (11/18/11), at 392-393; Arista User Manual</p>

Copyright Registration Information	Cisco	Arista
		v. 4.7.3 (7/18/11), at; Arista User Manual v. 4.7.3 (7/18/11), at 281-82.

Copyright Registration Information	Cisco	Arista																																																																																																																														
	<pre>switch# show spanning-tree mst</pre> <pre>##### MST0 vlans mapped: 1-4094 Bridge address 0019.bad7.fc15 priority 32768 (32768 sysid 0) Root this switch for the CIST Regional Root this switch Operational hello time 2 , forward delay 15, max age 20, txholdcount 6 Configured hello time 2 , forward delay 15, max age 20, max hops 20</pre> <table><thead><tr><th>Interface</th><th>Role</th><th>Sts</th><th>Cost</th><th>Prio.Nbr</th><th>Type</th></tr></thead><tbody><tr><td>Eth8/1</td><td>Desig FWD</td><td>20000</td><td>128</td><td>1025</td><td>P2p</td></tr><tr><td>Eth8/2</td><td>Desig FWD</td><td>20000</td><td>128</td><td>1026</td><td>P2p</td></tr></tbody></table> <p>This example shows how to display STP information about a specific MST instance:</p> <pre>switch# show spanning-tree mst 0</pre> <pre>##### MST0 vlans mapped: 1-4094 Bridge address 0019.bad7.fc15 priority 32768 (32768 sysid 0) Root this switch for the CIST Regional Root this switch Operational hello time 2 , forward delay 15, max age 20, txholdcount 6 Configured hello time 2 , forward delay 15, max age 20, max hops 20</pre> <table><thead><tr><th>Interface</th><th>Role</th><th>Sts</th><th>Cost</th><th>Prio.Nbr</th><th>Type</th></tr></thead><tbody><tr><td>Eth8/1</td><td>Desig FWD</td><td>20000</td><td>128</td><td>1025</td><td>P2p</td></tr><tr><td>Eth8/2</td><td>Desig FWD</td><td>20000</td><td>128</td><td>1026</td><td>P2p</td></tr></tbody></table> <p>This example shows how to display detailed STP information about the MST protocol:</p> <pre>switch# show spanning-tree mst detail</pre> <pre>##### MST0 vlans mapped: 1-4094 Bridge address 0019.bad7.fc15 priority 32768 (32768 sysid 0) Root this switch for the CIST Regional Root this switch Operational hello time 2 , forward delay 15, max age 20, txholdcount 6 Configured hello time 2 , forward delay 15, max age 20, max hops 20</pre> <pre>Eth8/1 of MST0 is designated forwarding Port info port id 128.1025 priority 128 cost 20000 Designated root address 0019.bad7.fc15 priority 32768 cost 0 Design. regional root address 0019.bad7.fc15 priority 32768 cost 0 Designated bridge address 0019.bad7.fc15 priority 32768 port id 128.1025 Timers: message expires in 0 sec, forward delay 0, forward transitions 1 Bpdus sent 1379, received 3</pre> <pre>Eth8/2 of MST0 is designated forwarding Port info port id 128.1026 priority 128 cost 20000 Designated root address 0019.bad7.fc15 priority 32768 cost 0 Design. regional root address 0019.bad7.fc15 priority 32768 cost 0 Designated bridge address 0019.bad7.fc15 priority 32768 port id 128.1026 Timers: message expires in 0 sec, forward delay 0, forward transitions 1 Bpdus sent 1380, received 2</pre>	Interface	Role	Sts	Cost	Prio.Nbr	Type	Eth8/1	Desig FWD	20000	128	1025	P2p	Eth8/2	Desig FWD	20000	128	1026	P2p	Interface	Role	Sts	Cost	Prio.Nbr	Type	Eth8/1	Desig FWD	20000	128	1025	P2p	Eth8/2	Desig FWD	20000	128	1026	P2p	<p>Examples</p> <ul style="list-style-type: none">This command displays interface data blocks for MST instance 3. <pre>switch# show spanning-tree mst 3 detail</pre> <pre>##### MST3 vlans mapped: 2 Bridge address 0011.2233.4402 priority 32771 (32768 sysid 3) Root address 0011.2233.4401 priority 32771 (32768 sysid 3)</pre> <pre>Ethernet1 of MST3 is root forwarding Port info port id 128.1 priority 128 cost 2000 Designated root address 0011.2233.4401 priority 32768 cost 0 Designated bridge address 0011.2233.4401 priority 32768 port id 128.1</pre> <pre>Ethernet2 of MST3 is alternate discarding Port info port id 128.2 priority 128 cost 2000 Designated root address 0011.2233.4401 priority 32768 cost 0 Designated bridge address 0011.2233.4401 priority 32768 port id 128.2</pre> <pre>Ethernet3 of MST3 is designated forwarding Port info port id 128.3 priority 128 cost 2000 Designated root address 0011.2233.4401 priority 32768 cost 2000 Designated bridge address 0011.2233.4402 priority 32768 port id 128.3</pre> <ul style="list-style-type: none">This command displays interface tables for all MST instances. <pre>switch# show spanning-tree mst</pre> <pre>##### MST0 vlans mapped: 1-4094 Bridge address 0011.2233.4402 priority 32768 (32768 sysid 0) Root address 0011.2233.4401 priority 32768 (32768 sysid 0) Regional Root address 0011.2233.4401 priority 32768 (32768 sysid 0)</pre> <table><thead><tr><th>Interface</th><th>Role</th><th>State</th><th>Cost</th><th>Prio.Nbr</th><th>Type</th></tr></thead><tbody><tr><td>E1</td><td>root</td><td>forwarding</td><td>2000</td><td>128.1</td><td>P2p</td></tr><tr><td>E2</td><td>alternate</td><td>discarding</td><td>2000</td><td>128.2</td><td>P2p</td></tr><tr><td>E3</td><td>designated</td><td>forwarding</td><td>2000</td><td>128.3</td><td>P2p</td></tr><tr><td>E4</td><td>designated</td><td>forwarding</td><td>2000</td><td>128.4</td><td>P2p</td></tr></tbody></table> <pre>##### MST2 vlans mapped: 2 Bridge address 0011.2233.4402 priority 8194 (8192 sysid 2) Root this switch for MST2</pre> <table><thead><tr><th>Interface</th><th>Role</th><th>State</th><th>Cost</th><th>Prio.Nbr</th><th>Type</th></tr></thead><tbody><tr><td>E1</td><td>designated</td><td>forwarding</td><td>2000</td><td>128.1</td><td>P2p</td></tr><tr><td>E2</td><td>designated</td><td>forwarding</td><td>2000</td><td>128.2</td><td>P2p</td></tr><tr><td>E3</td><td>designated</td><td>forwarding</td><td>2000</td><td>128.3</td><td>P2p</td></tr><tr><td>E4</td><td>designated</td><td>forwarding</td><td>2000</td><td>128.4</td><td>P2p</td></tr></tbody></table> <pre>##### MST3 vlans mapped: 3 Bridge address 0011.2233.4402 priority 32771 (32768 sysid 3) Root address 0011.2233.4401 priority 32771 (32768 sysid 3)</pre> <table><thead><tr><th>Interface</th><th>Role</th><th>State</th><th>Cost</th><th>Prio.Nbr</th><th>Type</th></tr></thead><tbody><tr><td>E1</td><td>root</td><td>forwarding</td><td>2000</td><td>128.1</td><td>P2p</td></tr><tr><td>E2</td><td>alternate</td><td>discarding</td><td>2000</td><td>128.2</td><td>P2p</td></tr><tr><td>E3</td><td>designated</td><td>forwarding</td><td>2000</td><td>128.3</td><td>P2p</td></tr><tr><td>E4</td><td>designated</td><td>forwarding</td><td>2000</td><td>128.4</td><td>P2p</td></tr></tbody></table>	Interface	Role	State	Cost	Prio.Nbr	Type	E1	root	forwarding	2000	128.1	P2p	E2	alternate	discarding	2000	128.2	P2p	E3	designated	forwarding	2000	128.3	P2p	E4	designated	forwarding	2000	128.4	P2p	Interface	Role	State	Cost	Prio.Nbr	Type	E1	designated	forwarding	2000	128.1	P2p	E2	designated	forwarding	2000	128.2	P2p	E3	designated	forwarding	2000	128.3	P2p	E4	designated	forwarding	2000	128.4	P2p	Interface	Role	State	Cost	Prio.Nbr	Type	E1	root	forwarding	2000	128.1	P2p	E2	alternate	discarding	2000	128.2	P2p	E3	designated	forwarding	2000	128.3	P2p	E4	designated	forwarding	2000	128.4	P2p
Interface	Role	Sts	Cost	Prio.Nbr	Type																																																																																																																											
Eth8/1	Desig FWD	20000	128	1025	P2p																																																																																																																											
Eth8/2	Desig FWD	20000	128	1026	P2p																																																																																																																											
Interface	Role	Sts	Cost	Prio.Nbr	Type																																																																																																																											
Eth8/1	Desig FWD	20000	128	1025	P2p																																																																																																																											
Eth8/2	Desig FWD	20000	128	1026	P2p																																																																																																																											
Interface	Role	State	Cost	Prio.Nbr	Type																																																																																																																											
E1	root	forwarding	2000	128.1	P2p																																																																																																																											
E2	alternate	discarding	2000	128.2	P2p																																																																																																																											
E3	designated	forwarding	2000	128.3	P2p																																																																																																																											
E4	designated	forwarding	2000	128.4	P2p																																																																																																																											
Interface	Role	State	Cost	Prio.Nbr	Type																																																																																																																											
E1	designated	forwarding	2000	128.1	P2p																																																																																																																											
E2	designated	forwarding	2000	128.2	P2p																																																																																																																											
E3	designated	forwarding	2000	128.3	P2p																																																																																																																											
E4	designated	forwarding	2000	128.4	P2p																																																																																																																											
Interface	Role	State	Cost	Prio.Nbr	Type																																																																																																																											
E1	root	forwarding	2000	128.1	P2p																																																																																																																											
E2	alternate	discarding	2000	128.2	P2p																																																																																																																											
E3	designated	forwarding	2000	128.3	P2p																																																																																																																											
E4	designated	forwarding	2000	128.4	P2p																																																																																																																											

Cisco NX-OS 5.0

Effective date of registration:
11/13/2014

Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2010), at L2-77

Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 990.

See also Arista User Manual v. 4.12.3 (7/17/13), at 867-68; Arista User Manual, v. 4.11.1 (1/11/13), at 685-86; Arista User Manual v. 4.10.3 (10/22/12), at 599-600; Arista User Manual v. 4.9.3.2 (5/3/12), at 518-19; Arista User Manual v. 4.8.2 (11/18/11), at 392-393; Arista User Manual v. 4.7.3 (7/18/11), at; Arista User Manual v. 4.7.3 (7/18/11), at 281-82.

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>This example shows how to display information about the MST configuration:</p> <pre>switch)# show spanning-tree mst configuration</pre> <pre> Name: [mst-bldg-sj6/3] Revision: 1 Instances Configured: 3 Instance Vlans mapped ----- 0 1 2000 2-2000 4094 2001-4094 ----- This example shows how to display the MD5 digest included in the current MST configuration:</pre> <pre>switch)# show spanning-tree mst configuration digest</pre> <pre> Name [mst-config] Revision 10 Instances configured 25 Digest 0x40D5ECA178C657835C83BBCE16723192 Pre-std Digest 0x27BF112A75B72781ED928D9EC5BE4251 </pre> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2013), at 81.</p>	<p>Examples</p> <ul style="list-style-type: none"> This command displays the MST region's VLAN-to-instance map. <pre>switch>show spanning-tree mst configuration</pre> <pre> Name [] Revision 0 Instances configured 3 Instance Vlans mapped ----- 0 1,4-4094 2 2 3 3 ----- switch> This command displays the MST region's configuration digest. <pre>switch>show spanning-tree mst configuration digest</pre> <pre> Name [] Revision 0 Instances configured 1 Digest 0xAC16177F50281CD4RR3R21D8AB26DR62 switch> </pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 991.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 869; Arista User Manual, v. 4.11.1 (1/11/13), at 687; Arista User Manual v. 4.10.3 (10/22/12), at 601; Arista User Manual v. 4.9.3.2 (5/3/12), at 520; Arista User Manual v. 4.8.2 (11/18/11), at 394; Arista User Manual v. 4.7.3 (7/18/11), at 283.</p> </pre>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 5.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>This example shows how to display information about the MST configuration:</p> <pre>switch)# show spanning-tree mst configuration</pre> <pre>Name: [mst-bldg-sj6/3] Revision: 1 Instances Configured: 3 Instance Vlans mapped ----- 0 1 2000 2-2000 4094 2001-4094 -----</pre> <p>This example shows how to display the MD5 digest included in the current MST configuration:</p> <pre>switch)# show spanning-tree mst configuration digest</pre> <pre>Name [mst-config] Revision 10 Instances configured 25 Digest 0x40D5ECA178C657835C83BBCB16723192 Pre-std Digest 0x27BF112A75B72781ED928D9EC5BE4251</pre> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2010), at L2-78</p>	<p>Examples</p> <ul style="list-style-type: none"> This command displays the MST region's VLAN-to-instance map. <pre>switch>show spanning-tree mst configuration</pre> <pre>Name [] Revision 0 Instances configured 3 Instance Vlans mapped ----- 0 1,4-4094 2 2 3 3 ----- switch></pre> <ul style="list-style-type: none"> This command displays the MST region's configuration digest. <pre>switch>show spanning-tree mst configuration digest</pre> <pre>Name [] Revision 0 Instances configured 1 Digest 0xAC16177F502A1CD4R3R21D8AB26DR62 switch></pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 991.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 869; Arista User Manual, v. 4.11.1 (1/11/13), at 687; Arista User Manual v. 4.10.3 (10/22/12), at 601; Arista User Manual v. 4.9.3.2 (5/3/12), at 520; Arista User Manual v. 4.8.2 (11/18/11), at 394; Arista User Manual v. 4.7.3 (7/18/11), at 283.</p>
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>Examples</p> <p>This example shows how to display information for the root bridge:</p> <pre>switch(config)# show spanning-tree root</pre> <pre>MST Instance Root ID Cost Time Age Dly Root Port ----- MST0000 32768 0018.bad7.fc15 0 2 20 15 This bridge is root</pre> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2013), at 82-83.</p>	<p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 994.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 872; Arista User Manual, v. 4.11.1 (1/11/13), at 690; Arista User Manual v. 4.10.3 (10/22/12), at 604; Arista User Manual v. 4.9.3.2 (5/3/12), at 523; Arista User Manual v. 4.8.2 (11/18/11), at 397; Arista User Manual v. 4.7.3 (7/18/11), at 286.</p>

Copyright Registration Information	Cisco	Arista														
Cisco NX-OS 5.0 Effective date of registration: 11/13/2014	<p>Examples</p> <p>This example shows how to display information for the root bridge:</p> <pre>switch(config)# show spanning-tree root</pre> <table><thead><tr><th>MST Instance</th><th>Root ID</th><th>Cost</th><th>Time</th><th>Age</th><th>Day</th><th>Root Port</th></tr></thead><tbody><tr><td>MST0000</td><td>32768</td><td>0018.ba07.fc15</td><td>0</td><td>2</td><td>20</td><td>15</td></tr></tbody></table> <p>This bridge is root</p> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2010), at L2-79:L2-80</p>	MST Instance	Root ID	Cost	Time	Age	Day	Root Port	MST0000	32768	0018.ba07.fc15	0	2	20	15	<p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 994.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 872; Arista User Manual, v. 4.11.1 (1/11/13), at 690; Arista User Manual v. 4.10.3 (10/22/12), at 604; Arista User Manual v. 4.9.3.2 (5/3/12), at 523; Arista User Manual v. 4.8.2 (11/18/11), at 397; Arista User Manual v. 4.7.3 (7/18/11), at 286.</p>
MST Instance	Root ID	Cost	Time	Age	Day	Root Port										
MST0000	32768	0018.ba07.fc15	0	2	20	15										
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<p>This example shows how to display information about the number of VLANs configured on the device:</p> <pre>switch# show vlan summary</pre> <pre>Number of existing VLANs : 9 Number of existing user VLANs : 9 Number of existing extended VLANs : 0</pre> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2013), at 94.</p>	<p>Example</p> <ul style="list-style-type: none">This command displays the number of VLANs on the switch. <pre>switch>show vlan summary Number of existing VLANs : 18 switch></pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 791.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 638; Arista User Manual, v. 4.11.1 (1/11/13), at 492; Arista User Manual v. 4.10.3 (10/22/12), at 410; Arista User Manual v. 4.9.3.2 (5/3/12), at 345.</p>														

Copyright Registration Information	Cisco	Arista																																
<p>Cisco NX-OS 5.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>This example shows how to display information about the number of VLANs configured on the device:</p> <pre>switch# show vlan summary</pre> <pre>Number of existing VLANs : 9 Number of existing user VLANs : 9 Number of existing extended VLANs : 0</pre> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 5.x (2010), at L2-90</p>	<p>Example</p> <ul style="list-style-type: none">This command displays the number of VLANs on the switch. <pre>switch>show vlan summary</pre> <pre>Number of existing VLANs : 18</pre> <pre>switch></pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 791.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 638; Arista User Manual, v. 4.11.1 (1/11/13), at 492; Arista User Manual v. 4.10.3 (10/22/12), at 410; Arista User Manual v. 4.9.3.2 (5/3/12), at 345.</p>																																
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>Examples</p> <p>This example shows how to display information about all private VLANs on the device:</p> <pre>switch(config)# show vlan private-vlan</pre> <table><thead><tr><th>Primary</th><th>Secondary</th><th>Type</th><th>Ports</th></tr></thead><tbody><tr><td>200</td><td>201</td><td>isolated</td><td>Eth2/26, Eth2/27</td></tr><tr><td>200</td><td>202</td><td>community</td><td>Eth2/26, Eth2/28</td></tr></tbody></table> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2013), at 94.</p>	Primary	Secondary	Type	Ports	200	201	isolated	Eth2/26, Eth2/27	200	202	community	Eth2/26, Eth2/28	<p>Example</p> <ul style="list-style-type: none">This command displays the private VLANs. <pre>switch>show vlan private-vlan</pre> <table><thead><tr><th>Primary</th><th>Secondary</th><th>Type</th><th>Ports</th></tr></thead><tbody><tr><td>5</td><td>25</td><td>isolated</td><td></td></tr><tr><td>5</td><td>26</td><td>isolated</td><td></td></tr><tr><td>7</td><td>31</td><td>community</td><td></td></tr><tr><td>7</td><td>32</td><td>isolated</td><td></td></tr></tbody></table> <pre>switch></pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 790.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 637; Arista User Manual, v. 4.11.1 (1/11/13), at 491; Arista User Manual v. 4.10.3 (10/22/12), at 409; Arista User Manual v. 4.9.3.2 (5/3/12), at 344.</p>	Primary	Secondary	Type	Ports	5	25	isolated		5	26	isolated		7	31	community		7	32	isolated	
Primary	Secondary	Type	Ports																															
200	201	isolated	Eth2/26, Eth2/27																															
200	202	community	Eth2/26, Eth2/28																															
Primary	Secondary	Type	Ports																															
5	25	isolated																																
5	26	isolated																																
7	31	community																																
7	32	isolated																																

Copyright Registration Information	Cisco	Arista																																
Cisco NX-OS 5.0 Effective date of registration: 11/13/2014	<p>Examples</p> <p>This example shows how to display information about all private VLANs on the device:</p> <pre>switch(config)# show vlan private-vlan</pre> <table><thead><tr><th>Primary</th><th>Secondary</th><th>Type</th><th>Ports</th></tr></thead><tbody><tr><td>200</td><td>201</td><td>isolated</td><td>Eth2/26, Eth2/27</td></tr><tr><td>200</td><td>202</td><td>community</td><td>Eth2/26, Eth2/28</td></tr></tbody></table> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2010), at L2-96</p>	Primary	Secondary	Type	Ports	200	201	isolated	Eth2/26, Eth2/27	200	202	community	Eth2/26, Eth2/28	<p>Example</p> <ul style="list-style-type: none">This command displays the private VLANs. <pre>switch>show vlan private-vlan</pre> <table><thead><tr><th>Primary</th><th>Secondary</th><th>Type</th><th>Ports</th></tr></thead><tbody><tr><td>5</td><td>25</td><td>isolated</td><td></td></tr><tr><td>5</td><td>26</td><td>isolated</td><td></td></tr><tr><td>7</td><td>31</td><td>community</td><td></td></tr><tr><td>7</td><td>32</td><td>isolated</td><td></td></tr></tbody></table> <pre>switch></pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 790.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 637; Arista User Manual, v. 4.11.1 (1/11/13), at 491; Arista User Manual v. 4.10.3 (10/22/12), at 409; Arista User Manual v. 4.9.3.2 (5/3/12), at 344.</p>	Primary	Secondary	Type	Ports	5	25	isolated		5	26	isolated		7	31	community		7	32	isolated	
	Primary	Secondary	Type	Ports																														
200	201	isolated	Eth2/26, Eth2/27																															
200	202	community	Eth2/26, Eth2/28																															
Primary	Secondary	Type	Ports																															
5	25	isolated																																
5	26	isolated																																
7	31	community																																
7	32	isolated																																
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<p>spanning-tree bpdupfilter</p> <p>To enable bridge protocol data unit (BPDU) Filtering on the interface, use the spanning-tree bpdupfilter command. To return to the default settings, use the no form of this command.</p> <pre>spanning-tree bpdupfilter {enable disable}</pre> <p>no spanning-tree bpdupfilter</p> <table><thead><tr><th>Syntax</th><th>Description</th></tr></thead><tbody><tr><td>enable</td><td>Enables BPDU Filtering on this interface.</td></tr><tr><td>disable</td><td>Disables BPDU Filtering on this interface.</td></tr></tbody></table> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2013), at 111.</p>	Syntax	Description	enable	Enables BPDU Filtering on this interface.	disable	Disables BPDU Filtering on this interface.	<p>spanning-tree bpdupfilter</p> <p>The spanning-tree bpdupfilter command controls bridge protocol data unit (BPDU) filtering on the configuration mode interface. BPDU filtering is disabled by default.</p> <p>Ports with BPDU filtering enabled drop inbound BPDUs and do not send BPDUs. Enabling BPDU filtering on a port not connected to a host can result in loops as the port continues forwarding data while ignoring inbound BPDU packets.</p> <ul style="list-style-type: none">spanning-tree bpdupfilter enabled enables BPDU filtering.spanning-tree bpdupfilter disabled disables BPDU filtering by removing the spanning-tree bpdupfilter command from running-config. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 996.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 874; Arista User Manual, v. 4.11.1 (1/11/13), at 692; Arista User Manual v. 4.10.3 (10/22/12), at 606; Arista User Manual v. 4.9.3.2 (5/3/12), at 525; Arista User Manual v. 4.8.2 (11/18/11), at 399; Arista User Manual v. 4.7.3 (7/18/11), at 265.</p>																										
Syntax	Description																																	
enable	Enables BPDU Filtering on this interface.																																	
disable	Disables BPDU Filtering on this interface.																																	

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>spanning-tree bridge assurance</p> <p>To enable Bridge Assurance on the device, use the <code>spanning-tree bridge assurance</code> command. To disable Bridge Assurance, use the <code>no</code> form of this command.</p> <p><code>spanning-tree bridge assurance</code> <code>no spanning-tree bridge assurance</code></p> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2013), at 115.</p>	<p>spanning-tree bridge assurance</p> <p>The <code>spanning-tree bridge assurance</code> command enables bridge assurance on all ports with a port type of <i>network</i>. Bridge assurance protects against unidirectional link failure, other software failure, and devices that quit running a spanning tree algorithm.</p> <p>Bridge assurance is available only on spanning tree <i>network</i> ports on point-to-point links. Both ends of the link must have bridge assurance enabled. If the device on one side of the link has bridge assurance enabled and the device on the other side either does not support bridge assurance or does not have it enabled, the bridge assurance enabled port is blocked.</p> <p>The <code>no spanning-tree bridge assurance</code> command disables bridge assurance.</p> <p>The <code>spanning-tree bridge assurance</code> and default <code>spanning-tree bridge assurance</code> commands restore the default behavior by removing the <code>no spanning-tree bridge assurance</code> command from <i>running-config</i>. Only the <code>no</code> form of this command is visible in <i>running-config</i>.</p> <p>Platform all Command Mode Global Configuration</p> <p>Command Syntax</p> <p><code>spanning-tree bridge assurance</code> <code>no spanning-tree bridge assurance</code> default <code>spanning-tree bridge assurance</code></p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 967.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 880; Arista User Manual, v. 4.11.1 (1/11/13), at 698; Arista User Manual v. 4.10.3 (10/22/12), at 612; Arista User Manual v. 4.9.3.2 (5/3/12), at 531; Arista User Manual v. 4.8.2 (11/18/11), at 403; Arista User Manual v. 4.7.3 (7/18/11), at 252.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 5.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>spanning-tree bridge assurance</p> <p>To enable Bridge Assurance on the device, use the <code>spanning-tree bridge assurance</code> command. To disable Bridge Assurance, use the <code>no</code> form of this command.</p> <p><code>spanning-tree bridge assurance</code> <code>no spanning-tree bridge assurance</code></p> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 5.x (2010), at L2-106.</p>	<p>spanning-tree bridge assurance</p> <p>The <code>spanning-tree bridge assurance</code> command enables bridge assurance on all ports with a port type of <i>network</i>. Bridge assurance protects against unidirectional link failure, other software failure, and devices that quit running a spanning tree algorithm.</p> <p>Bridge assurance is available only on spanning tree <i>network</i> ports on point-to-point links. Both ends of the link must have bridge assurance enabled. If the device on one side of the link has bridge assurance enabled and the device on the other side either does not support bridge assurance or does not have it enabled, the bridge assurance enabled port is blocked.</p> <p>The <code>no spanning-tree bridge assurance</code> command disables bridge assurance.</p> <p>The <code>spanning-tree bridge assurance</code> and default <code>spanning-tree bridge assurance</code> commands restore the default behavior by removing the <code>no spanning-tree bridge assurance</code> command from <i>running-config</i>. Only the <code>no</code> form of this command is visible in <i>running-config</i>.</p> <p>Platform all Command Mode Global Configuration</p> <p>Command Syntax</p> <p><code>spanning-tree bridge assurance</code> <code>no spanning-tree bridge assurance</code> default <code>spanning-tree bridge assurance</code></p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 967.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 880; Arista User Manual, v. 4.11.1 (1/11/13), at 698; Arista User Manual v. 4.10.3 (10/22/12), at 612; Arista User Manual v. 4.9.3.2 (5/3/12), at 531; Arista User Manual v. 4.8.2 (11/18/11), at 403; Arista User Manual v. 4.7.3 (7/18/11), at 252.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 4.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>spanning-tree bridge assurance</p> <p>To enable Bridge Assurance on the device, use the <code>spanning-tree bridge assurance</code> command. To disable Bridge Assurance, use the <code>no</code> form of this command.</p> <p><code>spanning-tree bridge assurance</code> <code>no spanning-tree bridge assurance</code></p> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 4.x (2008), at L2-33.</p>	<p>spanning-tree bridge assurance</p> <p>The <code>spanning-tree bridge assurance</code> command enables bridge assurance on all ports with a port type of <i>network</i>. Bridge assurance protects against unidirectional link failure, other software failure, and devices that quit running a spanning tree algorithm.</p> <p>Bridge assurance is available only on spanning tree <i>network</i> ports on point-to-point links. Both ends of the link must have bridge assurance enabled. If the device on one side of the link has bridge assurance enabled and the device on the other side either does not support bridge assurance or does not have it enabled, the bridge assurance enabled port is blocked.</p> <p>The <code>no spanning-tree bridge assurance</code> command disables bridge assurance.</p> <p>The <code>spanning-tree bridge assurance</code> and default <code>spanning-tree bridge assurance</code> commands restore the default behavior by removing the <code>no spanning-tree bridge assurance</code> command from <i>running-config</i>. Only the <code>no</code> form of this command is visible in <i>running-config</i>.</p> <p>Platform all Command Mode Global Configuration</p> <p>Command Syntax</p> <p><code>spanning-tree bridge assurance</code> <code>no spanning-tree bridge assurance</code> default <code>spanning-tree bridge assurance</code></p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 967.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 880; Arista User Manual, v. 4.11.1 (1/11/13), at 698; Arista User Manual v. 4.10.3 (10/22/12), at 612; Arista User Manual v. 4.9.3.2 (5/3/12), at 531; Arista User Manual v. 4.8.2 (11/18/11), at 403; Arista User Manual v. 4.7.3 (7/18/11), at 252.</p>

Copyright Registration Information	Cisco	Arista														
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>spanning-tree guard</p> <p>To enable or disable Loop Guard or Root Guard, use the <code>spanning-tree guard</code> command. To return to the default settings, use the <code>no</code> form of this command.</p> <p><code>spanning-tree guard {loop root none}</code></p> <p><code>no spanning-tree guard</code></p> <table border="1"> <tr> <td>Syntax Description</td><td>loop</td><td>Enables Loop Guard on the interface.</td></tr> <tr> <td></td><td>root</td><td>Enables Root Guard on the interface.</td></tr> <tr> <td></td><td>none</td><td>Sets the guard mode to none.</td></tr> </table> <p>Defaults Disabled</p> <p>Command Modes Interface configuration</p> <p>Supported User Roles network-admin vdc-admin</p> <table border="1"> <tr> <td rowspan="2">Command History</td><td>Release</td><td>Modification</td></tr> <tr> <td>4.0</td><td>This command was introduced.</td></tr> </table> <p>Usage Guidelines You cannot enable Loop Guard if Root Guard is enabled, although the device accepts the command to enable Loop Guard on spanning tree edge ports. This command does not require a license.</p> <p>Examples This example shows how to enable Root Guard:</p> <pre>switch(config-if)# spanning-tree guard root switch(config-if)#</pre> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, (2013), at 119.</p>	Syntax Description	loop	Enables Loop Guard on the interface.		root	Enables Root Guard on the interface.		none	Sets the guard mode to none.	Command History	Release	Modification	4.0	This command was introduced.	<p>spanning-tree guard</p> <p>The <code>spanning-tree guard</code> command enables root guard or loop guard on the configuration mode interface. The <code>spanning-tree loopguard default</code> command configures the global loop guard setting.</p> <ul style="list-style-type: none"> Root guard prevents a port from becoming a root or blocked port. A root guard port that receives a superior BPDU transitions to the root-inconsistent (blocked) state. Loop guard protects against loops resulting from unidirectional link failures on point-to-point links by preventing non-designated ports from becoming designated ports. When loop guard is enabled, a root or blocked port transitions to loop-inconsistent (blocked) state if it stops receiving BPDUs from its designated port. The port returns to its prior state when it receives a BPDU. <p>The <code>no spanning-tree guard</code> and default <code>spanning-tree guard</code> commands sets the configuration mode interface to the global loop guard mode by removing the <code>spanning-tree guard</code> statement from <i>running-config</i>. The <code>spanning-tree guard none</code> command disables loop guard and root guard on the interface, overriding the global setting.</p> <p>Platform all</p> <p>Command Mode Interface-Ethernet Configuration Interface-Port-Channel Configuration</p> <p>Command Syntax</p> <pre>spanning-tree guard PORT_MODE no spanning-tree guard default spanning-tree guard</pre> <p>Parameters</p> <ul style="list-style-type: none"> PORT_MODE the port mode. Options include: <ul style="list-style-type: none"> <code>loop</code> enables loop guard on the interface. <code>root</code> enables root guard on the interface. <code>none</code> disables root guard and loop guard. <p>Examples</p> <ul style="list-style-type: none"> This command enables root guard on Ethernet 5 interface. <pre>switch(config)#interface ethernet 5 switch(config-if-Et5)#spanning-tree guard root switch(config-if-Et5)#</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1005.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 883; Arista User Manual, v. 4.11.1 (1/11/13), at 701; Arista User Manual v. 4.10.3 (10/22/12), at 615; Arista User Manual v. 4.9.3.2 (5/3/12), at 534; Arista User Manual v. 4.8.2 (11/18/11), at 406; Arista User Manual v. 4.7.3 (7/18/11), at 268.</p>
Syntax Description	loop	Enables Loop Guard on the interface.														
	root	Enables Root Guard on the interface.														
	none	Sets the guard mode to none.														
Command History	Release	Modification														
	4.0	This command was introduced.														

Copyright Registration Information	Cisco	Arista															
<p>Cisco NX-OS 5.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>spanning-tree guard</p> <p>To enable or disable Loop Guard or Root Guard, use the <code>spanning-tree guard</code> command. To return to the default settings, use the <code>no</code> form of this command.</p> <p><code>spanning-tree guard {loop root none}</code></p> <p><code>no spanning-tree guard</code></p> <table border="1"> <tr> <td>Syntax Description</td><td>loop</td><td>Enables Loop Guard on the interface.</td></tr> <tr> <td></td><td>root</td><td>Enables Root Guard on the interface.</td></tr> <tr> <td></td><td>none</td><td>Sets the guard mode to none.</td></tr> </table> <p>Defaults Disabled</p> <p>Command Modes Interface configuration</p> <p>Supported User Roles network-admin vdc-admin</p> <table border="1"> <tr> <td>Command History</td><td>Release</td><td>Modification</td></tr> <tr> <td></td><td>4.0</td><td>This command was introduced.</td></tr> </table> <p>Usage Guidelines You cannot enable Loop Guard if Root Guard is enabled, although the device accepts the command to enable Loop Guard on spanning tree edge ports. This command does not require a license.</p> <p>Examples This example shows how to enable Root Guard:</p> <pre>switch(config-if)# spanning-tree guard root switch(config-if)#</pre> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 5.x (2010), at L-110.</p>	Syntax Description	loop	Enables Loop Guard on the interface.		root	Enables Root Guard on the interface.		none	Sets the guard mode to none.	Command History	Release	Modification		4.0	This command was introduced.	<p>spanning-tree guard</p> <p>The <code>spanning-tree guard</code> command enables root guard or loop guard on the configuration mode interface. The <code>spanning-tree loopguard default</code> command configures the global loop guard setting.</p> <ul style="list-style-type: none"> Root guard prevents a port from becoming a root or blocked port. A root guard port that receives a superior BPDU transitions to the root-inconsistent (blocked) state. Loop guard protects against loops resulting from unidirectional link failures on point-to-point links by preventing non-designated ports from becoming designated ports. When loop guard is enabled, a root or blocked port transitions to loop-inconsistent (blocked) state if it stops receiving BPDUs from its designated port. The port returns to its prior state when it receives a BPDU. <p>The <code>no spanning-tree guard</code> and default <code>spanning-tree guard</code> commands sets the configuration mode interface to the global loop guard mode by removing the <code>spanning-tree guard</code> statement from <i>running-config</i>. The <code>spanning-tree guard none</code> command disables loop guard and root guard on the interface, overriding the global setting.</p> <p>Platform all</p> <p>Command Mode Interface-Ethernet Configuration Interface-Port-Channel Configuration</p> <p>Command Syntax</p> <pre>spanning-tree guard PORT_MODE no spanning-tree guard default spanning-tree guard</pre> <p>Parameters</p> <ul style="list-style-type: none"> PORT_MODE the port mode. Options include: <ul style="list-style-type: none"> <code>loop</code> enables loop guard on the interface. <code>root</code> enables root guard on the interface. <code>none</code> disables root guard and loop guard. <p>Examples</p> <ul style="list-style-type: none"> This command enables root guard on Ethernet 5 interface. <pre>switch(config)#interface ethernet 5 switch(config-if-Et5)#spanning-tree guard root switch(config-if-Et5)#</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1005.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 883; Arista User Manual, v. 4.11.1 (1/11/13), at 701; Arista User Manual v. 4.10.3 (10/22/12), at 615; Arista User Manual v. 4.9.3.2 (5/3/12), at 534; Arista User Manual v. 4.8.2 (11/18/11), at 406; Arista User Manual v. 4.7.3 (7/18/11), at 268.</p>
Syntax Description	loop	Enables Loop Guard on the interface.															
	root	Enables Root Guard on the interface.															
	none	Sets the guard mode to none.															
Command History	Release	Modification															
	4.0	This command was introduced.															

Copyright Registration Information	Cisco	Arista															
<p>Cisco NX-OS 4.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>spanning-tree guard</p> <p>To enable or disable Loop Guard or Root Guard, use the <code>spanning-tree guard</code> command. To return to the default settings, use the <code>no</code> form of this command.</p> <p><code>spanning-tree guard {loop root none}</code></p> <p><code>no spanning-tree guard</code></p> <table border="1"> <tr> <td>Syntax Description</td><td>loop</td><td>Enables Loop Guard on the interface.</td></tr> <tr> <td></td><td>root</td><td>Enables Root Guard on the interface.</td></tr> <tr> <td></td><td>none</td><td>Sets the guard mode to none.</td></tr> </table> <p>Defaults Disabled</p> <p>Command Modes Interface configuration</p> <p>Supported User Roles network-admin vdc-admin</p> <table border="1"> <tr> <td>Command History</td><td>Release</td><td>Modification</td></tr> <tr> <td></td><td>4.0</td><td>This command was introduced.</td></tr> </table> <p>Usage Guidelines You cannot enable Loop Guard if Root Guard is enabled, although the device accepts the command to enable Loop Guard on spanning tree edge ports. This command does not require a license.</p> <p>Examples This example shows how to enable Root Guard:</p> <pre>switch(config-if)# spanning-tree guard root switch(config-if)#</pre> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 4.x (2008), at L-37.</p>	Syntax Description	loop	Enables Loop Guard on the interface.		root	Enables Root Guard on the interface.		none	Sets the guard mode to none.	Command History	Release	Modification		4.0	This command was introduced.	<p>spanning-tree guard</p> <p>The <code>spanning-tree guard</code> command enables root guard or loop guard on the configuration mode interface. The <code>spanning-tree loopguard default</code> command configures the global loop guard setting.</p> <ul style="list-style-type: none"> Root guard prevents a port from becoming a root or blocked port. A root guard port that receives a superior BPDU transitions to the root-inconsistent (blocked) state. Loop guard protects against loops resulting from unidirectional link failures on point-to-point links by preventing non-designated ports from becoming designated ports. When loop guard is enabled, a root or blocked port transitions to loop-inconsistent (blocked) state if it stops receiving BPDUs from its designated port. The port returns to its prior state when it receives a BPDU. <p>The <code>no spanning-tree guard</code> and default <code>spanning-tree guard</code> commands sets the configuration mode interface to the global loop guard mode by removing the <code>spanning-tree guard</code> statement from <i>running-config</i>. The <code>spanning-tree guard none</code> command disables loop guard and root guard on the interface, overriding the global setting.</p> <p>Platform all</p> <p>Command Mode Interface-Ethernet Configuration Interface-Port-Channel Configuration</p> <p>Command Syntax</p> <pre>spanning-tree guard PORT_MODE no spanning-tree guard default spanning-tree guard</pre> <p>Parameters</p> <ul style="list-style-type: none"> PORT_MODE the port mode. Options include: <ul style="list-style-type: none"> <code>loop</code> enables loop guard on the interface. <code>root</code> enables root guard on the interface. <code>none</code> disables root guard and loop guard. <p>Examples</p> <ul style="list-style-type: none"> This command enables root guard on Ethernet 5 interface. <pre>switch(config)#interface ethernet 5 switch(config-if-Et5)#spanning-tree guard root switch(config-if-Et5)#</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1005.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 883; Arista User Manual, v. 4.11.1 (1/11/13), at 701; Arista User Manual v. 4.10.3 (10/22/12), at 615; Arista User Manual v. 4.9.3.2 (5/3/12), at 534; Arista User Manual v. 4.8.2 (11/18/11), at 406; Arista User Manual v. 4.7.3 (7/18/11), at 268.</p>
Syntax Description	loop	Enables Loop Guard on the interface.															
	root	Enables Root Guard on the interface.															
	none	Sets the guard mode to none.															
Command History	Release	Modification															
	4.0	This command was introduced.															

Copyright Registration Information	Cisco	Arista
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<p>To enable Loop Guard as a default on all ports of a given bridge, use the spanning-tree loopguard default command. To disable Loop Guard, use the no form of this command.</p> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, (2013), at 121.</p>	<ul style="list-style-type: none"> spanning-tree loopguard default command enables loop guard as a default on all switch ports. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 996.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 844; Arista User Manual, v. 4.11.1 (1/11/13), at 662; Arista User Manual v. 4.10.3 (10/22/12), 576; Arista User Manual v. 4.9.3.2 (5/3/12), at 496; Arista User Manual v. 4.8.2 (11/18/11), at 370; Arista User Manual v. 4.7.3 (7/18/11), at 255.</p>
Cisco NX-OS 5.0 Effective date of registration: 11/13/2014	<p>To enable Loop Guard as a default on all ports of a given bridge, use the spanning-tree loopguard default command. To disable Loop Guard, use the no form of this command.</p> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 5.x (2010), at L2-112.</p>	<ul style="list-style-type: none"> spanning-tree loopguard default command enables loop guard as a default on all switch ports. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 996.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 844; Arista User Manual, v. 4.11.1 (1/11/13), at 662; Arista User Manual v. 4.10.3 (10/22/12), 576; Arista User Manual v. 4.9.3.2 (5/3/12), at 496; Arista User Manual v. 4.8.2 (11/18/11), at 370; Arista User Manual v. 4.7.3 (7/18/11), at 255.</p>
Cisco NX-OS 4.0 Effective date of registration: 11/13/2014	<p>To enable Loop Guard as a default on all ports of a given bridge, use the spanning-tree loopguard default command. To disable Loop Guard, use the no form of this command.</p> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 4.x (2008), at L2-39.</p>	<ul style="list-style-type: none"> spanning-tree loopguard default command enables loop guard as a default on all switch ports. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 996.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 844; Arista User Manual, v. 4.11.1 (1/11/13), at 662; Arista User Manual v. 4.10.3 (10/22/12), 576; Arista User Manual v. 4.9.3.2 (5/3/12), at 496; Arista User Manual v. 4.8.2 (11/18/11), at 370; Arista User Manual v. 4.7.3 (7/18/11), at 255.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>spanning-tree loopguard default</p> <p>To enable Loop Guard as a default on all ports of a given bridge, use the <code>spanning-tree loopguard default</code> command. To disable Loop Guard, use the <code>no</code> form of this command.</p> <p><code>spanning-tree loopguard default</code></p> <p><code>no spanning-tree loopguard default</code></p> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, (2013), at 121.</p>	<p>spanning-tree loopguard default</p> <p>The <code>spanning-tree loopguard default</code> command configures the global loop guard setting as <i>enabled</i>. Ports not covered by a <code>spanning-tree guard</code> command use the global loop guard setting. Loop guard prevents blocked or root ports from becoming a designated port due to failures resulting in a unidirectional link. The <code>spanning-tree guard</code> interface configuration statement overrides the global setting for a specified interface. The default global loop guard setting is <i>disabled</i>.</p> <p>The <code>no spanning-tree loopguard default</code> and <code>default spanning-tree loopguard default</code> commands restore the global loop guard setting of <i>disabled</i> by removing the <code>spanning-tree loopguard default</code> command from <i>running-config</i>.</p> <p>Platform all Command Mode Global Configuration</p> <p>Command Syntax</p> <p><code>spanning-tree loopguard default</code> <code>no spanning-tree loopguard default</code> <code>default spanning-tree loopguard default</code></p> <p>Examples</p> <ul style="list-style-type: none"> This command enables loop guard as the default on all switch ports. <pre>switch(config)#spanning-tree loopguard default switch(config)#</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1008.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 886; Arista User Manual, v. 4.11.1 (1/11/13), at 704; Arista User Manual v. 4.10.3 (10/22/12), at 618; Arista User Manual v. 4.9.3.2 (5/3/12), at 537; Arista User Manual v. 4.8.2 (11/18/11), at 409; Arista User Manual v. 4.7.3 (7/18/11), at 255.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 5.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>spanning-tree loopguard default</p> <p>To enable Loop Guard as a default on all ports of a given bridge, use the <code>spanning-tree loopguard default</code> command. To disable Loop Guard, use the <code>no</code> form of this command.</p> <p><code>spanning-tree loopguard default</code></p> <p><code>no spanning-tree loopguard default</code></p> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 5.x (2010), at L2-112.</p>	<p>spanning-tree loopguard default</p> <p>The <code>spanning-tree loopguard default</code> command configures the global loop guard setting as <i>enabled</i>. Ports not covered by a <code>spanning-tree guard</code> command use the global loop guard setting. Loop guard prevents blocked or root ports from becoming a designated port due to failures resulting in a unidirectional link. The <code>spanning-tree guard</code> interface configuration statement overrides the global setting for a specified interface. The default global loop guard setting is <i>disabled</i>.</p> <p>The <code>no spanning-tree loopguard default</code> and <code>default spanning-tree loopguard default</code> commands restore the global loop guard setting of <i>disabled</i> by removing the <code>spanning-tree loopguard default</code> command from <i>running-config</i>.</p> <p>Platform all Command Mode Global Configuration</p> <p>Command Syntax</p> <p><code>spanning-tree loopguard default</code> <code>no spanning-tree loopguard default</code> <code>default spanning-tree loopguard default</code></p> <p>Examples</p> <ul style="list-style-type: none"> This command enables loop guard as the default on all switch ports. <pre>switch(config)#spanning-tree loopguard default switch(config)#</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1008.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 886; Arista User Manual, v. 4.11.1 (1/11/13), at 704; Arista User Manual v. 4.10.3 (10/22/12), at 618; Arista User Manual v. 4.9.3.2 (5/3/12), at 537; Arista User Manual v. 4.8.2 (11/18/11), at 409; Arista User Manual v. 4.7.3 (7/18/11), at 255.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 4.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>spanning-tree loopguard default</p> <p>To enable Loop Guard as a default on all ports of a given bridge, use the <code>spanning-tree loopguard default</code> command. To disable Loop Guard, use the <code>no</code> form of this command.</p> <p><code>spanning-tree loopguard default</code></p> <p><code>no spanning-tree loopguard default</code></p> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 4.x (2008), at L2-39.</p>	<p>spanning-tree loopguard default</p> <p>The <code>spanning-tree loopguard default</code> command configures the global loop guard setting as <i>enabled</i>. Ports not covered by a <code>spanning-tree guard</code> command use the global loop guard setting. Loop guard prevents blocked or root ports from becoming a designated port due to failures resulting in a unidirectional link. The <code>spanning-tree guard</code> interface configuration statement overrides the global setting for a specified interface. The default global loop guard setting is <i>disabled</i>.</p> <p>The <code>no spanning-tree loopguard default</code> and <code>default spanning-tree loopguard default</code> commands restore the global loop guard setting of <i>disabled</i> by removing the <code>spanning-tree loopguard default</code> command from <i>running-config</i>.</p> <p>Platform all Command Mode Global Configuration</p> <p>Command Syntax</p> <p><code>spanning-tree loopguard default</code> <code>no spanning-tree loopguard default</code> <code>default spanning-tree loopguard default</code></p> <p>Examples</p> <ul style="list-style-type: none"> This command enables loop guard as the default on all switch ports. <pre>switch(config)#spanning-tree loopguard default switch(config)#</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1008.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 886; Arista User Manual, v. 4.11.1 (1/11/13), at 704; Arista User Manual v. 4.10.3 (10/22/12), at 618; Arista User Manual v. 4.9.3.2 (5/3/12), at 537; Arista User Manual v. 4.8.2 (11/18/11), at 409; Arista User Manual v. 4.7.3 (7/18/11), at 255.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>spanning-tree mst configuration</p> <p>To enter the Multiple Spanning Tree (MST) configuration submode, use the <code>spanning-tree mst configuration</code> command. To return to the default settings, use the <code>no</code> form of this command.</p> <p><code>spanning-tree mst configuration</code> <code>no spanning-tree mst configuration</code></p> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, (2013), , at 124.</p>	<p>spanning-tree mst configuration</p> <p>The <code>spanning-tree mst configuration</code> command places the switch in MST-configuration mode, which is the group change mode where MST region parameters are configured.</p> <p>Changes made in a group change mode are saved by leaving the mode through the <code>exit</code> command or by entering another configuration mode. To discard changes from the current edit session, leave the mode with the <code>abort</code> command.</p> <p>These commands are available in MST-configuration mode:</p> <ul style="list-style-type: none"> • <code>abort (mst-configuration mode)</code> • <code>exit (mst-configuration mode)</code> • <code>instance</code> • <code>name (mst-configuration mode)</code> • <code>revision (mst-configuration mode)</code> • <code>show (mst-configuration mode)</code> <p>The <code>no spanning-tree mst configuration</code> and default <code>spanning-tree mst configuration</code> commands restore the MST default configuration.</p> <p>Platform all Command Mode Global Configuration</p> <p>Command Syntax</p> <p><code>spanning-tree mst configuration</code> <code>no spanning-tree mst configuration</code> default <code>spanning-tree mst configuration</code></p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1012.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 890; Arista User Manual, v. 4.11.1 (1/11/13), at 708; Arista User Manual v. 4.10.3 (10/22/12), at 612; Arista User Manual v. 4.9.3.2 (5/3/12), at 541; Arista User Manual v. 4.8.2 (11/18/11), at 413.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 5.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>spanning-tree mst configuration</p> <p>To enter the Multiple Spanning Tree (MST) configuration submode, use the <code>spanning-tree mst configuration</code> command. To return to the default settings, use the <code>no</code> form of this command.</p> <p><code>spanning-tree mst configuration</code> <code>no spanning-tree mst configuration</code></p> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 5.x (2010), at L2-115.</p>	<p>spanning-tree mst configuration</p> <p>The <code>spanning-tree mst configuration</code> command places the switch in MST-configuration mode, which is the group change mode where MST region parameters are configured.</p> <p>Changes made in a group change mode are saved by leaving the mode through the <code>exit</code> command or by entering another configuration mode. To discard changes from the current edit session, leave the mode with the <code>abort</code> command.</p> <p>These commands are available in MST-configuration mode:</p> <ul style="list-style-type: none"> • <code>abort (mst-configuration mode)</code> • <code>exit (mst-configuration mode)</code> • <code>instance</code> • <code>name (mst-configuration mode)</code> • <code>revision (mst-configuration mode)</code> • <code>show (mst-configuration mode)</code> <p>The <code>no spanning-tree mst configuration</code> and default <code>spanning-tree mst configuration</code> commands restore the MST default configuration.</p> <p>Platform all Command Mode Global Configuration</p> <p>Command Syntax</p> <p><code>spanning-tree mst configuration</code> <code>no spanning-tree mst configuration</code> default <code>spanning-tree mst configuration</code></p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1012.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 890; Arista User Manual, v. 4.11.1 (1/11/13), at 708; Arista User Manual v. 4.10.3 (10/22/12), at 612; Arista User Manual v. 4.9.3.2 (5/3/12), at 541; Arista User Manual v. 4.8.2 (11/18/11), at 413.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 4.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>spanning-tree mst configuration</p> <p>To enter the Multiple Spanning Tree (MST) configuration submode, use the <code>spanning-tree mst configuration</code> command. To return to the default settings, use the <code>no</code> form of this command.</p> <p><code>spanning-tree mst configuration</code> <code>no spanning-tree mst configuration</code></p> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 4.x (2008), at L2-42.</p>	<p>spanning-tree mst configuration</p> <p>The <code>spanning-tree mst configuration</code> command places the switch in MST-configuration mode, which is the group change mode where MST region parameters are configured.</p> <p>Changes made in a group change mode are saved by leaving the mode through the <code>exit</code> command or by entering another configuration mode. To discard changes from the current edit session, leave the mode with the <code>abort</code> command.</p> <p>These commands are available in MST-configuration mode:</p> <ul style="list-style-type: none"> • <code>abort (mst-configuration mode)</code> • <code>exit (mst-configuration mode)</code> • <code>instance</code> • <code>name (mst-configuration mode)</code> • <code>revision (mst-configuration mode)</code> • <code>show (mst-configuration mode)</code> <p>The <code>no spanning-tree mst configuration</code> and default <code>spanning-tree mst configuration</code> commands restore the MST default configuration.</p> <p>Platform all Command Mode Global Configuration</p> <p>Command Syntax</p> <p><code>spanning-tree mst configuration</code> <code>no spanning-tree mst configuration</code> <code>default spanning-tree mst configuration</code></p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1012.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 890; Arista User Manual, v. 4.11.1 (1/11/13), at 708; Arista User Manual v. 4.10.3 (10/22/12), at 612; Arista User Manual v. 4.9.3.2 (5/3/12), at 541; Arista User Manual v. 4.8.2 (11/18/11), at 413.</p>

Copyright Registration Information	Cisco	Arista															
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<table border="1"> <thead> <tr> <th>Related Commands</th><th>Command</th><th>Description</th></tr> </thead> <tbody> <tr> <td></td><td><code>instance vlan</code></td><td>Maps a VLAN or a set of VLANs to an MST instance.</td></tr> <tr> <td></td><td><code>name (mst configuration)</code></td><td>Sets the name of an MST region.</td></tr> <tr> <td></td><td><code>revision</code></td><td>Sets the revision number for the MST configuration.</td></tr> <tr> <td></td><td><code>show spanning-tree mst</code></td><td>Displays information about the MST protocol.</td></tr> </tbody> </table> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2013), at 125.</p>	Related Commands	Command	Description		<code>instance vlan</code>	Maps a VLAN or a set of VLANs to an MST instance.		<code>name (mst configuration)</code>	Sets the name of an MST region.		<code>revision</code>	Sets the revision number for the MST configuration.		<code>show spanning-tree mst</code>	Displays information about the MST protocol.	<p>The <code>instance</code> command inserts an entry into the VLAN-to-instance map that associates a set of VLANs to an MST instance. In addition to defining the MST topology, the VLAN-to-instance map is one of three parameters, along with the MST name and revision number, that identifies the switch's MST region.</p> <p>The <code>no instance</code> command removes specified entries from the VLAN-to-instance map. If the command does not provide a VLAN list, all entries are removed for the specified instance. The <code>no instance</code> and <code>default instance</code> commands function identically.</p> <p>Platform all Command Mode MST-Configuration</p> <p>Command Syntax</p> <pre>instance mst_inst vlans v_range no instance mst_inst [vlans v_range] no default instance mst_inst [vlans v_range]</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 978.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 856; Arista User Manual, v. 4.11.1 (1/11/13), at 674; Arista User Manual v. 4.10.3 (10/22/12), at 588; Arista User Manual v. 4.9.3.2 (5/3/12), at 507; Arista User Manual v. 4.8.2 (11/18/11), at 381; Arista User Manual v. 4.7.3 (7/18/11), at 293.</p>
Related Commands	Command	Description															
	<code>instance vlan</code>	Maps a VLAN or a set of VLANs to an MST instance.															
	<code>name (mst configuration)</code>	Sets the name of an MST region.															
	<code>revision</code>	Sets the revision number for the MST configuration.															
	<code>show spanning-tree mst</code>	Displays information about the MST protocol.															

Copyright Registration Information	Cisco	Arista															
<p>Cisco NX-OS 5.0</p> <p>Effective date of registration: 11/13/2014</p>	<table border="1"> <thead> <tr> <th>Related Commands</th><th>Command</th><th>Description</th></tr> </thead> <tbody> <tr> <td></td><td><code>instance vlan</code></td><td>Maps a VLAN or a set of VLANs to an MST instance.</td></tr> <tr> <td></td><td><code>name (mst configuration)</code></td><td>Sets the name of an MST region.</td></tr> <tr> <td></td><td><code>revision</code></td><td>Sets the revision number for the MST configuration.</td></tr> <tr> <td></td><td><code>show spanning-tree mst</code></td><td>Displays information about the MST protocol.</td></tr> </tbody> </table> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 5.x (2010), at L2-116.</p>	Related Commands	Command	Description		<code>instance vlan</code>	Maps a VLAN or a set of VLANs to an MST instance.		<code>name (mst configuration)</code>	Sets the name of an MST region.		<code>revision</code>	Sets the revision number for the MST configuration.		<code>show spanning-tree mst</code>	Displays information about the MST protocol.	<p>The <code>instance</code> command inserts an entry into the VLAN-to-instance map that associates a set of VLANs to an MST instance. In addition to defining the MST topology, the VLAN-to-instance map is one of three parameters, along with the MST name and revision number, that identifies the switch's MST region.</p> <p>The <code>no instance</code> command removes specified entries from the VLAN-to-instance map. If the command does not provide a VLAN list, all entries are removed for the specified instance. The <code>no instance</code> and <code>default instance</code> commands function identically.</p> <p>Platform all Command Mode MST-Configuration</p> <p>Command Syntax</p> <pre>instance mst_inst vlans v_range no instance mst_inst [vlans v_range] no default instance mst_inst [vlans v_range]</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 978.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 856; Arista User Manual, v. 4.11.1 (1/11/13), at 674; Arista User Manual v. 4.10.3 (10/22/12), at 588; Arista User Manual v. 4.9.3.2 (5/3/12), at 507; Arista User Manual v. 4.8.2 (11/18/11), at 381; Arista User Manual v. 4.7.3 (7/18/11), at 293.</p>
Related Commands	Command	Description															
	<code>instance vlan</code>	Maps a VLAN or a set of VLANs to an MST instance.															
	<code>name (mst configuration)</code>	Sets the name of an MST region.															
	<code>revision</code>	Sets the revision number for the MST configuration.															
	<code>show spanning-tree mst</code>	Displays information about the MST protocol.															

Copyright Registration Information	Cisco	Arista															
<p>Cisco NX-OS 4.0</p> <p>Effective date of registration: 11/13/2014</p>	<table border="1"> <thead> <tr> <th>Related Commands</th><th>Command</th><th>Description</th></tr> </thead> <tbody> <tr> <td></td><td><code>instance vlan</code></td><td>Maps a VLAN or a set of VLANs to an MST instance.</td></tr> <tr> <td></td><td><code>name (mst configuration)</code></td><td>Sets the name of an MST region.</td></tr> <tr> <td></td><td><code>revision</code></td><td>Sets the revision number for the MST configuration.</td></tr> <tr> <td></td><td><code>show spanning-tree mst</code></td><td>Displays information about the MST protocol.</td></tr> </tbody> </table> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 4.x (2008), at L2-43.</p>	Related Commands	Command	Description		<code>instance vlan</code>	Maps a VLAN or a set of VLANs to an MST instance.		<code>name (mst configuration)</code>	Sets the name of an MST region.		<code>revision</code>	Sets the revision number for the MST configuration.		<code>show spanning-tree mst</code>	Displays information about the MST protocol.	<p>The <code>instance</code> command inserts an entry into the VLAN-to-instance map that associates a set of VLANs to an MST instance. In addition to defining the MST topology, the VLAN-to-instance map is one of three parameters, along with the MST name and revision number, that identifies the switch's MST region.</p> <p>The <code>no instance</code> command removes specified entries from the VLAN-to-instance map. If the command does not provide a VLAN list, all entries are removed for the specified instance. The <code>no instance</code> and <code>default instance</code> commands function identically.</p> <p>Platform all Command Mode MST-Configuration</p> <p>Command Syntax</p> <pre>instance mst_inst vlans v_range no instance mst_inst [vlans v_range] no default instance mst_inst [vlans v_range]</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 978.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 856; Arista User Manual, v. 4.11.1 (1/11/13), at 674; Arista User Manual v. 4.10.3 (10/22/12), at 588; Arista User Manual v. 4.9.3.2 (5/3/12), at 507; Arista User Manual v. 4.8.2 (11/18/11), at 381; Arista User Manual v. 4.7.3 (7/18/11), at 293.</p>
Related Commands	Command	Description															
	<code>instance vlan</code>	Maps a VLAN or a set of VLANs to an MST instance.															
	<code>name (mst configuration)</code>	Sets the name of an MST region.															
	<code>revision</code>	Sets the revision number for the MST configuration.															
	<code>show spanning-tree mst</code>	Displays information about the MST protocol.															





Copyright Registration Information	Cisco	Arista															
<p>Cisco IOS 15.1</p> <p>Effective date of registration: 11/28/2014</p>	<table border="1"> <thead> <tr> <th>Related Commands</th><th>Command</th><th>Description</th></tr> </thead> <tbody> <tr> <td></td><td><code>instance vlan</code></td><td>Maps a VLAN or a set of VLANs to an MST instance.</td></tr> <tr> <td></td><td><code>name (mst configuration)</code></td><td>Sets the name of an MST region.</td></tr> <tr> <td></td><td><code>revision</code></td><td>Sets the revision number for the MST configuration.</td></tr> <tr> <td></td><td><code>show spanning-tree mst</code></td><td>Displays information about the MST protocol.</td></tr> </tbody> </table> <p>Cisco IOS Configuration Fundamentals Command Reference (2010), at CF-488:CF-489.</p>	Related Commands	Command	Description		<code>instance vlan</code>	Maps a VLAN or a set of VLANs to an MST instance.		<code>name (mst configuration)</code>	Sets the name of an MST region.		<code>revision</code>	Sets the revision number for the MST configuration.		<code>show spanning-tree mst</code>	Displays information about the MST protocol.	<p>The <code>instance</code> command inserts an entry into the VLAN-to-instance map that associates a set of VLANs to an MST instance. In addition to defining the MST topology, the VLAN-to-instance map is one of three parameters, along with the MST name and revision number, that identifies the switch's MST region.</p> <p>The <code>no instance</code> command removes specified entries from the VLAN-to-instance map. If the command does not provide a VLAN list, all entries are removed for the specified instance. The <code>no instance</code> and <code>default instance</code> commands function identically.</p> <p>Platform all Command Mode MST-Configuration</p> <p>Command Syntax</p> <pre>instance mst_inst vlans v_range no instance mst_inst [vlans v_range] no default instance mst_inst [vlans v_range]</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 978.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 856; Arista User Manual, v. 4.11.1 (1/11/13), at 674; Arista User Manual v. 4.10.3 (10/22/12), at 588; Arista User Manual v. 4.9.3.2 (5/3/12), at 507; Arista User Manual v. 4.8.2 (11/18/11), at 381; Arista User Manual v. 4.7.3 (7/18/11), at 293.</p>
Related Commands	Command	Description															
	<code>instance vlan</code>	Maps a VLAN or a set of VLANs to an MST instance.															
	<code>name (mst configuration)</code>	Sets the name of an MST region.															
	<code>revision</code>	Sets the revision number for the MST configuration.															
	<code>show spanning-tree mst</code>	Displays information about the MST protocol.															



Copyright Registration Information	Cisco	Arista															
<p>Cisco IOS XE 2.1</p> <p>Effective date of registration: 11/24/2014</p>	<table border="1"> <thead> <tr> <th>Related Commands</th><th>Command</th><th>Description</th></tr> </thead> <tbody> <tr> <td></td><td><code>instance vlan</code></td><td>Maps a VLAN or a set of VLANs to an MST instance.</td></tr> <tr> <td></td><td><code>name (mst configuration)</code></td><td>Sets the name of an MST region.</td></tr> <tr> <td></td><td><code>revision</code></td><td>Sets the revision number for the MST configuration.</td></tr> <tr> <td></td><td><code>show spanning-tree mst</code></td><td>Displays information about the MST protocol.</td></tr> </tbody> </table> <p>Cisco IOS Configuration Fundamentals Command Reference (2008), at CF-466:CF467.</p>	Related Commands	Command	Description		<code>instance vlan</code>	Maps a VLAN or a set of VLANs to an MST instance.		<code>name (mst configuration)</code>	Sets the name of an MST region.		<code>revision</code>	Sets the revision number for the MST configuration.		<code>show spanning-tree mst</code>	Displays information about the MST protocol.	<p>The <code>instance</code> command inserts an entry into the VLAN-to-instance map that associates a set of VLANs to an MST instance. In addition to defining the MST topology, the VLAN-to-instance map is one of three parameters, along with the MST name and revision number, that identifies the switch's MST region.</p> <p>The <code>no instance</code> command removes specified entries from the VLAN-to-instance map. If the command does not provide a VLAN list, all entries are removed for the specified instance. The <code>no instance</code> and <code>default instance</code> commands function identically.</p> <p>Platform all Command Mode MST-Configuration</p> <p>Command Syntax</p> <pre>instance mst_inst vlans v_range no instance mst_inst [vlans v_range] no default instance mst_inst [vlans v_range]</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 978.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 856; Arista User Manual, v. 4.11.1 (1/11/13), at 674; Arista User Manual v. 4.10.3 (10/22/12), at 588; Arista User Manual v. 4.9.3.2 (5/3/12), at 507; Arista User Manual v. 4.8.2 (11/18/11), at 381; Arista User Manual v. 4.7.3 (7/18/11), at 293.</p>
Related Commands	Command	Description															
	<code>instance vlan</code>	Maps a VLAN or a set of VLANs to an MST instance.															
	<code>name (mst configuration)</code>	Sets the name of an MST region.															
	<code>revision</code>	Sets the revision number for the MST configuration.															
	<code>show spanning-tree mst</code>	Displays information about the MST protocol.															

Copyright Registration Information	Cisco	Arista																
<div>Cisco NX-OS 6.2</div> <div>Effective date of registration: 11/13/2014</div>	<table><tr><th>Related Commands</th><th>Command</th><th>Description</th></tr><tr><td></td><td>show spanning-tree summary</td><td>Displays information about the spanning tree configuration.</td></tr><tr><td></td><td>spanning-tree bpduguard</td><td>Enables BPDU Guard on the interface.</td></tr><tr><td></td><td>spanning-tree port type edge</td><td>Configures an interface as a spanning tree edge port.</td></tr></table> <div>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2013), at 148.</div>	Related Commands	Command	Description		show spanning-tree summary	Displays information about the spanning tree configuration.		spanning-tree bpduguard	Enables BPDU Guard on the interface.		spanning-tree port type edge	Configures an interface as a spanning tree edge port.	<div>spanning-tree bpduguard</div> <div>The spanning-tree bpduguard command controls BPDU guard on the configuration mode interface. A BPDU guard-enabled port is disabled when it receives a BPDU packet. Disabled ports differ from blocked ports in that they are re-enabled only through manual intervention.</div> <div>The BPDU guard default setting for portfast ports is configured by the spanning-tree portfast bpduguard default command; BPDU guard is disabled by default on all non-portfast ports.</div> <div><ul style="list-style-type: none">spanning-tree bpduguard enable enables BPDU guard on the interface.spanning-tree bpduguard disable disables BPDU guard on the interface.</div> <div>The no spanning-tree bpduguard and default spanning-tree bpduguard commands restore the global BPDU guard setting on the configuration mode interface by removing the corresponding spanning-tree bpduguard command from running-config.</div> <table><tr><td>Platform</td><td>all</td></tr><tr><td>Command Mode</td><td>Interface-Ethernet Configuration Interface-Port-Channel Configuration</td></tr></table> <div>Command Syntax</div> <div>spanning-tree bpduguard GUARD_ACTION no spanning-tree bpduguard default spanning-tree bpduguard</div> <div>Parameters</div> <div><ul style="list-style-type: none">GUARD_ACTION BPDU guard setting. Options include:<ul style="list-style-type: none">enabled BPDU guard is enabled on the interface.disabled BPDU guard is disabled on the interface.</div> <div>Examples</div> <div><ul style="list-style-type: none">These commands enable BPDU guard on Ethernet interface 5.<pre>switch(config)#interface ethernet 5 switch(config-if-Et5)#spanning-tree bpduguard enabled switch(config-if-Et5)</pre></div> <div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 997.</div> <div>See also Arista User Manual v. 4.12.3 (7/17/13), at 875; Arista User Manual, v. 4.11.1 (1/11/13), at 693; Arista User Manual v. 4.10.3 (10/22/12), at 607; Arista User Manual v. 4.9.3.2 (5/3/12), at 526; Arista User Manual v. 4.8.2 (11/18/11), at 400; Arista User Manual v. 4.7.3 (7/18/11), at 266.</div>	Platform	all	Command Mode	Interface-Ethernet Configuration Interface-Port-Channel Configuration
	Related Commands	Command	Description															
		show spanning-tree summary	Displays information about the spanning tree configuration.															
	spanning-tree bpduguard	Enables BPDU Guard on the interface.																
	spanning-tree port type edge	Configures an interface as a spanning tree edge port.																
Platform	all																	
Command Mode	Interface-Ethernet Configuration Interface-Port-Channel Configuration																	

Copyright Registration Information	Cisco	Arista																
<div>Cisco NX-OS 5.0</div> <div>Effective date of registration: 11/13/2014</div>	<table><tr><th>Related Commands</th><th>Command</th><th>Description</th></tr><tr><td></td><td>show spanning-tree summary</td><td>Displays information about the spanning tree configuration.</td></tr><tr><td></td><td>spanning-tree bpduguard</td><td>Enables BPDU Guard on the interface.</td></tr><tr><td></td><td>spanning-tree port type edge</td><td>Configures an interface as a spanning tree edge port.</td></tr></table> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 5.x (2010), at L2-138.</p>	Related Commands	Command	Description		show spanning-tree summary	Displays information about the spanning tree configuration.		spanning-tree bpduguard	Enables BPDU Guard on the interface.		spanning-tree port type edge	Configures an interface as a spanning tree edge port.	<p>spanning-tree bpduguard</p> <p>The spanning-tree bpduguard command controls BPDU guard on the configuration mode interface. A BPDU guard-enabled port is disabled when it receives a BPDU packet. Disabled ports differ from blocked ports in that they are re-enabled only through manual intervention.</p> <p>The BPDU guard default setting for portfast ports is configured by the spanning-tree portfast bpduguard default command; BPDU guard is disabled by default on all non-portfast ports.</p> <ul style="list-style-type: none">spanning-tree bpduguard enable enables BPDU guard on the interface.spanning-tree bpduguard disable disables BPDU guard on the interface. <p>The no spanning-tree bpduguard and default spanning-tree bpduguard commands restore the global BPDU guard setting on the configuration mode interface by removing the corresponding spanning-tree bpduguard command from <i>running-config</i>.</p> <table><tr><td>Platform</td><td>all</td></tr><tr><td>Command Mode</td><td>Interface-Ethernet Configuration Interface-Port-Channel Configuration</td></tr></table> <p>Command Syntax</p> <pre>spanning-tree bpduguard <i>GUARD_ACTION</i> no spanning-tree bpduguard default spanning-tree bpduguard</pre> <p>Parameters</p> <ul style="list-style-type: none"><i>GUARD_ACTION</i> BPDU guard setting. Options include:<ul style="list-style-type: none">enabled BPDU guard is enabled on the interface.disabled BPDU guard is disabled on the interface. <p>Examples</p> <ul style="list-style-type: none">These commands enable BPDU guard on Ethernet interface 5.<pre>switch(config)#interface ethernet 5 switch(config-if-Et5)#spanning-tree bpduguard enabled switch(config-if-Et5)</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 997.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 875; Arista User Manual, v. 4.11.1 (1/11/13), at 693; Arista User Manual v. 4.10.3 (10/22/12), at 607; Arista User Manual v. 4.9.3.2 (5/3/12), at 526; Arista User Manual v. 4.8.2 (11/18/11), at 400; Arista User Manual v. 4.7.3 (7/18/11), at 266.</p>	Platform	all	Command Mode	Interface-Ethernet Configuration Interface-Port-Channel Configuration
	Related Commands	Command	Description															
		show spanning-tree summary	Displays information about the spanning tree configuration.															
	spanning-tree bpduguard	Enables BPDU Guard on the interface.																
	spanning-tree port type edge	Configures an interface as a spanning tree edge port.																
Platform	all																	
Command Mode	Interface-Ethernet Configuration Interface-Port-Channel Configuration																	

Copyright Registration Information	Cisco	Arista																
<div>Cisco NX-OS 4.0</div> <div>Effective date of registration: 11/13/2014</div>	<table><tr><th>Related Commands</th><th>Command</th><th>Description</th></tr><tr><td></td><td>show spanning-tree summary</td><td>Displays information about the spanning tree configuration.</td></tr><tr><td></td><td>spanning-tree bpduguard</td><td>Enables BPDU Guard on the interface.</td></tr><tr><td></td><td>spanning-tree port type edge</td><td>Configures an interface as a spanning tree edge port.</td></tr></table> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 4.x (2008), at L2-65.</p>	Related Commands	Command	Description		show spanning-tree summary	Displays information about the spanning tree configuration.		spanning-tree bpduguard	Enables BPDU Guard on the interface.		spanning-tree port type edge	Configures an interface as a spanning tree edge port.	<p>spanning-tree bpduguard</p> <p>The spanning-tree bpduguard command controls BPDU guard on the configuration mode interface. A BPDU guard-enabled port is disabled when it receives a BPDU packet. Disabled ports differ from blocked ports in that they are re-enabled only through manual intervention.</p> <p>The BPDU guard default setting for portfast ports is configured by the spanning-tree portfast bpduguard default command; BPDU guard is disabled by default on all non-portfast ports.</p> <ul style="list-style-type: none">spanning-tree bpduguard enable enables BPDU guard on the interface.spanning-tree bpduguard disable disables BPDU guard on the interface. <p>The no spanning-tree bpduguard and default spanning-tree bpduguard commands restore the global BPDU guard setting on the configuration mode interface by removing the corresponding spanning-tree bpduguard command from <i>running-config</i>.</p> <table><tr><td>Platform</td><td>all</td></tr><tr><td>Command Mode</td><td>Interface-Ethernet Configuration Interface-Port-Channel Configuration</td></tr></table> <p>Command Syntax</p> <pre>spanning-tree bpduguard <i>GUARD_ACTION</i> no spanning-tree bpduguard default spanning-tree bpduguard</pre> <p>Parameters</p> <ul style="list-style-type: none"><i>GUARD_ACTION</i> BPDU guard setting. Options include:<ul style="list-style-type: none">enabled BPDU guard is enabled on the interface.disabled BPDU guard is disabled on the interface. <p>Examples</p> <ul style="list-style-type: none">These commands enable BPDU guard on Ethernet interface 5.<pre>switch(config)#interface ethernet 5 switch(config-if-Et5)#spanning-tree bpduguard enabled switch(config-if-Et5)</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 997.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 875; Arista User Manual, v. 4.11.1 (1/11/13), at 693; Arista User Manual v. 4.10.3 (10/22/12), at 607; Arista User Manual v. 4.9.3.2 (5/3/12), at 526; Arista User Manual v. 4.8.2 (11/18/11), at 400; Arista User Manual v. 4.7.3 (7/18/11), at 266.</p>	Platform	all	Command Mode	Interface-Ethernet Configuration Interface-Port-Channel Configuration
	Related Commands	Command	Description															
		show spanning-tree summary	Displays information about the spanning tree configuration.															
	spanning-tree bpduguard	Enables BPDU Guard on the interface.																
	spanning-tree port type edge	Configures an interface as a spanning tree edge port.																
Platform	all																	
Command Mode	Interface-Ethernet Configuration Interface-Port-Channel Configuration																	

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p> Caution When disabling spanning tree on a VLAN using the <code>no spanning-tree vlan <i>vlan-id</i></code> command, ensure that all switches and bridges in the VLAN have spanning tree disabled. You cannot disable spanning tree on some switches and bridges in a VLAN and leave it enabled on other switches and bridges in the same VLAN because switches and bridges with spanning tree enabled have incomplete information about the physical topology of the network.</p> <p> Caution We do not recommend disabling spanning tree even in a topology that is free of physical loops. Spanning tree is a safeguard against misconfigurations and cabling errors. Do not disable spanning tree in a VLAN without ensuring that there are no physical loops present in the VLAN.</p> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2013), at 159.</p>	<p>Warning Disabling spanning tree is not recommended, even in topologies free of physical loops. Spanning tree guards against configuration mistakes and cabling errors. When disabling VLAN, ensure that there are no physical loops in the VLAN.</p> <p>Important When disabling spanning tree on a VLAN, ensure that all switches and bridges in the network disable spanning tree for the same VLAN. Disabling spanning tree on a subset of switches and bridges in a VLAN may have unexpected results because switches and bridges running spanning tree will have incomplete information regarding the network's physical topology.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1023.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 901; Arista User Manual, v. 4.11.1 (1/11/13), at 719; Arista User Manual v. 4.10.3 (10/22/12), at 633; Arista User Manual v. 4.9.3.2 (5/3/12), at 550; Arista User Manual v. 4.8.2 (11/18/11), at 422; Arista User Manual v. 4.7.3 (7/18/11), at 264.</p>
<p>Cisco NX-OS 5.0</p> <p>Effective date of registration: 11/13/2014</p>	<p> Caution When disabling spanning tree on a VLAN using the <code>no spanning-tree vlan <i>vlan-id</i></code> command, ensure that all switches and bridges in the VLAN have spanning tree disabled. You cannot disable spanning tree on some switches and bridges in a VLAN and leave it enabled on other switches and bridges in the same VLAN because switches and bridges with spanning tree enabled have incomplete information about the physical topology of the network.</p> <p> Caution We do not recommend disabling spanning tree even in a topology that is free of physical loops. Spanning tree is a safeguard against misconfigurations and cabling errors. Do not disable spanning tree in a VLAN without ensuring that there are no physical loops present in the VLAN.</p> <p>Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, Release 5.x (2010), at L2-150.</p>	<p>Warning Disabling spanning tree is not recommended, even in topologies free of physical loops. Spanning tree guards against configuration mistakes and cabling errors. When disabling VLAN, ensure that there are no physical loops in the VLAN.</p> <p>Important When disabling spanning tree on a VLAN, ensure that all switches and bridges in the network disable spanning tree for the same VLAN. Disabling spanning tree on a subset of switches and bridges in a VLAN may have unexpected results because switches and bridges running spanning tree will have incomplete information regarding the network's physical topology.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1023.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 901; Arista User Manual, v. 4.11.1 (1/11/13), at 719; Arista User Manual v. 4.10.3 (10/22/12), at 633; Arista User Manual v. 4.9.3.2 (5/3/12), at 550; Arista User Manual v. 4.8.2 (11/18/11), at 422; Arista User Manual v. 4.7.3 (7/18/11), at 264.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 4.0</p> <p>Effective date of registration: 11/13/2014</p>	<div data-bbox="310 282 1134 415">  <p>Caution When disabling spanning tree on a VLAN using the <code>no spanning-tree vlan <i>vlan-id</i></code> command, ensure that all switches and bridges in the VLAN have spanning tree disabled. You cannot disable spanning tree on some switches and bridges in a VLAN and leave it enabled on other switches and bridges in the same VLAN because switches and bridges with spanning tree enabled have incomplete information about the physical topology of the network.</p> </div> <div data-bbox="310 435 1134 532">  <p>Caution We do not recommend disabling spanning tree even in a topology that is free of physical loops. Spanning tree is a safeguard against misconfigurations and cabling errors. Do not disable spanning tree in a VLAN without ensuring that there are no physical loops present in the VLAN.</p> </div> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 4.x (2008), at L2-75.</p>	<div data-bbox="1182 282 2032 350"> <p>Warning Disabling spanning tree is not recommended, even in topologies free of physical loops. Spanning tree guards against configuration mistakes and cabling errors. When disabling VLAN, ensure that there are no physical loops in the VLAN.</p> </div> <div data-bbox="1182 386 2032 470"> <p>Important When disabling spanning tree on a VLAN, ensure that all switches and bridges in the network disable spanning tree for the same VLAN. Disabling spanning tree on a subset of switches and bridges in a VLAN may have unexpected results because switches and bridges running spanning tree will have incomplete information regarding the network's physical topology.</p> </div> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1023.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 901; Arista User Manual, v. 4.11.1 (1/11/13), at 719; Arista User Manual v. 4.10.3 (10/22/12), at 633; Arista User Manual v. 4.9.3.2 (5/3/12), at 550; Arista User Manual v. 4.8.2 (11/18/11), at 422; Arista User Manual v. 4.7.3 (7/18/11), at 264.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>switchport private-vlan trunk native vlan</p> <p>To set the native VLAN for private VLAN promiscuous and isolated trunk ports, use the <code>switchport private-vlan trunk native vlan</code> command. To return to the default value, use the <code>no</code> form of this command.</p> <p><code>switchport private-vlan trunk native vlan vlan-id</code></p> <p><code>no switchport private-vlan trunk native vlan vlan-id</code></p> <p>Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, Release 5.x (2010), 177.</p>	<p>switchport trunk native vlan</p> <p>The <code>switchport trunk native vlan</code> command specifies the trunk mode native VLAN for the configuration mode interface. Interfaces in trunk mode associate untagged frames with the native VLAN. Trunk mode interfaces can also be configured to drop untagged frames. The default native VLAN for all interfaces is VLAN 1.</p> <p>The <code>no switchport trunk native vlan</code> and <code>default switchport trunk native vlan</code> commands restore VLAN 1 as the trunk mode native VLAN to the configuration mode interface by removing the corresponding <code>switchport trunk native vlan</code> command from <i>running-config</i>.</p> <p>Platform all Command Mode Interface-Ethernet Configuration Interface-Port-channel Configuration</p> <p>Command Syntax</p> <p><code>switchport trunk native vlan VLAN_ID</code> <code>no switchport trunk native vlan</code> <code>default switchport trunk native vlan</code></p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 800.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 647; Arista User Manual, v. 4.11.1 (1/11/13), at 500; Arista User Manual v. 4.10.3 (10/22/12), at 418; Arista User Manual v. 4.9.3.2 (5/3/12), at 357.</p>

Copyright Registration Information	Cisco	Arista															
Cisco NX-OS 5.0 Effective date of registration: 11/13/2014	<div>switchport private-vlan trunk native vlan</div> <p>To set the native VLAN for private VLAN promiscuous and isolated trunk ports, use the switchport private-vlan trunk native vlan command. To return to the default value, use the no form of this command.</p> <div>switchport private-vlan trunk native vlan vlan-id</div> <div>no switchport private-vlan trunk native vlan vlan-id</div> <p>Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, Release 5.x (2010), at L2-168.</p>	<div>switchport trunk native vlan</div> <p>The switchport trunk native vlan command specifies the trunk mode native VLAN for the configuration mode interface. Interfaces in trunk mode associate untagged frames with the native VLAN. Trunk mode interfaces can also be configured to drop untagged frames. The default native VLAN for all interfaces is VLAN 1.</p> <p>The no switchport trunk native vlan and default switchport trunk native vlan commands restore VLAN 1 as the trunk mode native VLAN to the configuration mode interface by removing the corresponding switchport trunk native vlan command from running-config.</p> <table><tr><td>Platform</td><td>all</td></tr><tr><td>Command Mode</td><td>Interface-Ethernet Configuration Interface-Port-channel Configuration</td></tr></table> <p>Command Syntax</p> <div>switchport trunk native vlan VLAN_ID</div> <div>no switchport trunk native vlan</div> <div>default switchport trunk native vlan</div> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 800.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 647; Arista User Manual, v. 4.11.1 (1/11/13), at 500; Arista User Manual v. 4.10.3 (10/22/12), at 418; Arista User Manual v. 4.9.3.2 (5/3/12), at 357.</p>	Platform	all	Command Mode	Interface-Ethernet Configuration Interface-Port-channel Configuration											
	Platform	all															
Command Mode	Interface-Ethernet Configuration Interface-Port-channel Configuration																
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<table><tr><td>Syntax Description</td><td>add</td><td>(Optional) Adds a VLAN to the current list.</td></tr><tr><td></td><td>except</td><td>(Optional) Specifies all VLANs except a particular VLAN.</td></tr><tr><td></td><td>none</td><td>(Optional) Specifies no VLANs.</td></tr><tr><td></td><td>remove</td><td>(Optional) Removes the VLANs from the current list.</td></tr><tr><td></td><td>vlan-id</td><td>VLAN ID. The range is from 2 to 1001.</td></tr></table> <p>Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, Release 6.x (2013), at 179.</p>	Syntax Description	add	(Optional) Adds a VLAN to the current list.		except	(Optional) Specifies all VLANs except a particular VLAN.		none	(Optional) Specifies no VLANs.		remove	(Optional) Removes the VLANs from the current list.		vlan-id	VLAN ID. The range is from 2 to 1001.	<p>Parameters</p> <ul style="list-style-type: none">EDIT_ACTION modifications to the VLAN list.<ul style="list-style-type: none">v_range Creates VLAN list from v_range.add v_range Adds specified VLANs to current list.all VLAN list contains all VLANs.except v_range VLAN list contains all VLANs except those specified.none VLAN list is empty (no VLANs).remove v_range Removes specified VLANs from current list. <p>Valid v_range formats include number (1 to 4094), range, or comma-delimited list of numbers and ranges.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 751.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 599; Arista User Manual, v. 4.11.1 (1/11/13), at 480; Arista User Manual v. 4.10.3 (10/22/12), at 399; Arista User Manual v. 4.9.3.2 (5/3/12), at 355.</p>
Syntax Description	add	(Optional) Adds a VLAN to the current list.															
	except	(Optional) Specifies all VLANs except a particular VLAN.															
	none	(Optional) Specifies no VLANs.															
	remove	(Optional) Removes the VLANs from the current list.															
	vlan-id	VLAN ID. The range is from 2 to 1001.															

Copyright Registration Information	Cisco	Arista						
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<p>area stub (OSPF)</p> <p>To define an area as an Open Shortest Path First (OSPF) stub area, use the <code>area stub</code> command. To remove the area, use the <code>no</code> form of this command.</p> <pre>area area-id stub [no-summary] no area area-id stub [no-summary]</pre> <table><tr><th>Syntax</th><th>Description</th></tr><tr><td><code>area-id</code></td><td>Identifier for the OSPF stub area. Specify as either a positive integer value or an IP address.</td></tr><tr><td><code>no-summary</code></td><td>(Optional) Prevents an Area Border Router (ABR) from sending summary link advertisements into the stub area.</td></tr></table> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference (2013), at 42.</p>	Syntax	Description	<code>area-id</code>	Identifier for the OSPF stub area. Specify as either a positive integer value or an IP address.	<code>no-summary</code>	(Optional) Prevents an Area Border Router (ABR) from sending summary link advertisements into the stub area.	<p>no area (OSPFv3)</p> <p>The <code>no area</code> command removes all area configuration commands for the specified OSPFv3 area. Commands removed by the <code>no area</code> command include:</p> <ul style="list-style-type: none">• <code>area</code>• <code>nssa</code>• <code>range</code>• <code>stub</code> <p>Area settings can be removed individually; refer to the command description page of the desired command for details.</p> <p>Platform all Command Mode Router-OSPF3 Configuration</p> <p>Command Syntax</p> <pre>no area area_id [TYPE] default area area_id [TYPE]</pre> <p>Parameters</p> <ul style="list-style-type: none">• <code>area_id</code> area number. Valid formats: integer <1 to 4294967295> or dotted decimal <0.0.0.1 to 255.255.255.255> Area 0 (or 0.0.0.0) is not configurable; it is always <i>normal</i>. <i>Running-config</i> stores value in dotted decimal notation.• <code>TYPE</code> area type. Values include:<ul style="list-style-type: none">— <code>nssa</code>— <code>nssa translate type7 always</code> sets p-bit when sending type 7 LSAs— <code>stub</code>— <code>stub no-summary</code> Prevents ABRs from sending summary link advertisements into the area. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/24/2014), at 1521.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1305; Arista User Manual, v. 4.11.1 (1/11/13), at 1056; Arista User Manual v. 4.10.3 (10/22/12), at 781.</p>
	Syntax	Description						
<code>area-id</code>	Identifier for the OSPF stub area. Specify as either a positive integer value or an IP address.							
<code>no-summary</code>	(Optional) Prevents an Area Border Router (ABR) from sending summary link advertisements into the stub area.							

Copyright Registration Information	Cisco	Arista						
Cisco NX-OS 5.0 Effective date of registration: 11/13/2014	<p>area stub (OSPF)</p> <p>To define an area as an Open Shortest Path First (OSPF) stub area, use the <code>area stub</code> command. To remove the area, use the <code>no</code> form of this command.</p> <pre>area area-id stub [no-summary] no area area-id stub [no-summary]</pre> <table><tr><th>Syntax</th><th>Description</th></tr><tr><td>area-id</td><td>Identifier for the OSPF stub area. Specify as either a positive integer value or an IP address.</td></tr><tr><td>no-summary</td><td>(Optional) Prevents an Area Border Router (ABR) from sending summary link advertisements into the stub area.</td></tr></table> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 5.x (2010), at L3-34.</p>	Syntax	Description	area-id	Identifier for the OSPF stub area. Specify as either a positive integer value or an IP address.	no-summary	(Optional) Prevents an Area Border Router (ABR) from sending summary link advertisements into the stub area.	<p>no area (OSPFv3)</p> <p>The <code>no area</code> command removes all area configuration commands for the specified OSPFv3 area. Commands removed by the <code>no area</code> command include:</p> <ul style="list-style-type: none">• <code>area</code>• <code>nssa</code>• <code>range</code>• <code>stub</code> <p>Area settings can be removed individually; refer to the command description page of the desired command for details.</p> <p>Platform all Command Mode Router-OSPF3 Configuration</p> <p>Command Syntax</p> <pre>no area area_id [TYPE] default area area_id [TYPE]</pre> <p>Parameters</p> <ul style="list-style-type: none">• <code>area_id</code> area number. Valid formats: integer <1 to 4294967295> or dotted decimal <0.0.0.1 to 255.255.255.255> Area 0 (or 0.0.0.0) is not configurable; it is always <i>normal</i>. <i>Running-config</i> stores value in dotted decimal notation.• <code>TYPE</code> area type. Values include:<ul style="list-style-type: none">— <code>nssa</code>— <code>nssa translate type7 always</code> sets p-bit when sending type 7 LSAs— <code>stub</code>— <code>stub no-summary</code> Prevents ABRs from sending summary link advertisements into the area. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/24/2014), at 1521.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1305; Arista User Manual, v. 4.11.1 (1/11/13), at 1056; Arista User Manual v. 4.10.3 (10/22/12), at 781.</p>
	Syntax	Description						
area-id	Identifier for the OSPF stub area. Specify as either a positive integer value or an IP address.							
no-summary	(Optional) Prevents an Area Border Router (ABR) from sending summary link advertisements into the stub area.							

Copyright Registration Information	Cisco	Arista						
Cisco NX-OS 4.0 Effective date of registration: 11/13/2014	<p>area stub (OSPF)</p> <p>To define an area as an Open Shortest Path First (OSPF) stub area, use the <code>area stub</code> command. To remove the area, use the <code>no</code> form of this command.</p> <pre>area area-id stub [no-summary] no area area-id stub [no-summary]</pre> <table><tr><th>Syntax</th><th>Description</th></tr><tr><td><code>area-id</code></td><td>Identifier for the OSPF stub area. Specify as either a positive integer value or an IP address.</td></tr><tr><td><code>no-summary</code></td><td>(Optional) Prevents an Area Border Router (ABR) from sending summary link advertisements into the stub area.</td></tr></table> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 4.x (2008), at L3-32.</p>	Syntax	Description	<code>area-id</code>	Identifier for the OSPF stub area. Specify as either a positive integer value or an IP address.	<code>no-summary</code>	(Optional) Prevents an Area Border Router (ABR) from sending summary link advertisements into the stub area.	<p>no area (OSPFv3)</p> <p>The <code>no area</code> command removes all area configuration commands for the specified OSPFv3 area. Commands removed by the <code>no area</code> command include:</p> <ul style="list-style-type: none">• <code>area</code>• <code>nssa</code>• <code>range</code>• <code>stub</code> <p>Area settings can be removed individually; refer to the command description page of the desired command for details.</p> <p>Platform all Command Mode Router-OSPF3 Configuration</p> <p>Command Syntax</p> <pre>no area area_id [TYPE] default area area_id [TYPE]</pre> <p>Parameters</p> <ul style="list-style-type: none">• <code>area_id</code> area number. Valid formats: integer <1 to 4294967295> or dotted decimal <0.0.0.1 to 255.255.255.255> Area 0 (or 0.0.0.0) is not configurable; it is always <i>normal</i>. <i>Running-config</i> stores value in dotted decimal notation.• <code>TYPE</code> area type. Values include:<ul style="list-style-type: none">— <code>nssa</code>— <code>nssa translate type7 always</code> sets p-bit when sending type 7 LSAs— <code>stub</code>— <code>stub no-summary</code> Prevents ABRs from sending summary link advertisements into the area. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/24/2014), at 1521.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1305; Arista User Manual, v. 4.11.1 (1/11/13), at 1056; Arista User Manual v. 4.10.3 (10/22/12), at 781.</p>
	Syntax	Description						
<code>area-id</code>	Identifier for the OSPF stub area. Specify as either a positive integer value or an IP address.							
<code>no-summary</code>	(Optional) Prevents an Area Border Router (ABR) from sending summary link advertisements into the stub area.							

Copyright Registration Information	Cisco	Arista						
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<p>This example shows how to clear all OSPF neighbor details for all OSPF instances:</p> <pre>switch# clear ip ospf neighbor *</pre> <p>This example shows how to clear all OSPF neighbor details for all neighbors on Ethernet interface 1/2 for OSPF instance 202:</p> <pre>switch# clear ip ospf 202 neighbor ethernet 1/2</pre> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference (2013), at 112.</p>	<p>Examples</p> <ul style="list-style-type: none">This command resets all OSPF neighbor statistics. <pre>switch#clear ip ospf neighbor * switch#</pre> <ul style="list-style-type: none">This command resets the OSPF neighbor statistics for the specified Ethernet 3 interface. <pre>switch#clear ip ospf neighbor ethernet 3 switch##</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1420.</p>						
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<p>default-information originate (OSPF)</p> <p>To generate a default external route into an Open Shortest Path First (OSPF) routing domain, use the default-information originate command. To disable this feature, use the no form of this command.</p> <pre>default-information originate [always] [route-map map-name] no default-information originate [always] [route-map map-name]</pre> <table><tr><th>Syntax</th><th>Description</th></tr><tr><td>always</td><td>(Optional) Specifies to always advertise the default route regardless of whether the route table has a default route.</td></tr><tr><td>route-map map-name</td><td>(Optional) Specifies to advertise the default route if the route map is satisfied. The map-name argument can be any alphanumeric string up to 63 characters.</td></tr></table> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference (2013), at 42.</p>	Syntax	Description	always	(Optional) Specifies to always advertise the default route regardless of whether the route table has a default route.	route-map map-name	(Optional) Specifies to advertise the default route if the route map is satisfied. The map-name argument can be any alphanumeric string up to 63 characters.	<p>Examples</p> <ul style="list-style-type: none">These commands will always advertise the OSPFv2 default route regardless of whether the switch has a default route configured. <pre>switch(config)#router ospf 1 switch((config-router-ospf)#default-information originate always switch(config-router-ospf)#show active router ospf 1 default-information originate always</pre> <ul style="list-style-type: none">These commands advertise a default route with a metric of 100 and an external metric type of 1 if a default route is configured. <pre>switch(config)#router ospf 1 switch((config-router-ospf)#default-information originate metric 100 metric-type 1</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1423.</p>
Syntax	Description							
always	(Optional) Specifies to always advertise the default route regardless of whether the route table has a default route.							
route-map map-name	(Optional) Specifies to advertise the default route if the route map is satisfied. The map-name argument can be any alphanumeric string up to 63 characters.							

Copyright Registration Information	Cisco	Arista						
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<h3>default-information originate (OSPFv3)</h3> <p>To generate a default external route into an Open Shortest Path First version 3 (OSPFv3) routing domain, use the default-information originate command. To disable this feature, use the no form of this command.</p> <pre>default-information originate [always] [route-map map-name] no default-information originate [always] [route-map map-name]</pre> <table><tr><td>Syntax Description</td><td>always</td><td>(Optional) Specifies to always advertise the default route regardless of whether the route table has a default route.</td></tr><tr><td></td><td>route-map map-name</td><td>(Optional) Specifies to advertise the default route if the route map is satisfied. The <i>map-name</i> argument can be any alphanumeric string up to 63 characters.</td></tr></table> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference (2013), at 44.</p>	Syntax Description	always	(Optional) Specifies to always advertise the default route regardless of whether the route table has a default route.		route-map map-name	(Optional) Specifies to advertise the default route if the route map is satisfied. The <i>map-name</i> argument can be any alphanumeric string up to 63 characters.	<h3>Examples</h3> <ul style="list-style-type: none">These commands will always advertise the OSPFv3 default route regardless of whether the switch has a default route configured.<pre>switch(config)#ipv6 router ospf 1 switch(config-router-ospf3)#default-information originate always switch(config-router-ospf3)#show active ipv6 router ospf 1 default-information originate always</pre>These commands configures OSPF area 1 as metric of 100 for the default route with an external metric type of Type 1.<pre>switch(config)#ipv6 router ospf 1 switch(config-router-ospf3)#default-information originate metric 100 metric-type 1 switch(config-router-ospf3)#show active ipv6 router ospf 1 default-information originate metric 100 metric-type 1 switch(config-router-ospf3)#</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1506.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1291; Arista User Manual, v. 4.11.1 (1/11/13), at 1041.</p>
	Syntax Description	always	(Optional) Specifies to always advertise the default route regardless of whether the route table has a default route.					
	route-map map-name	(Optional) Specifies to advertise the default route if the route map is satisfied. The <i>map-name</i> argument can be any alphanumeric string up to 63 characters.						

Copyright Registration Information	Cisco	Arista						
Cisco NX-OS 5.0 Effective date of registration: 11/13/2014	<div>default-information originate (OSPFv3)</div> <div>To generate a default external route into an Open Shortest Path First version 3 (OSPFv3) routing domain, use the default-information originate command. To disable this feature, use the no form of this command.</div> <div>default-information originate [always] [route-map map-name]</div> <div>no default-information originate [always] [route-map map-name]</div> <div><table><tr><td>Syntax Description</td><td>always</td><td>(Optional) Specifies to always advertise the default route regardless of whether the route table has a default route.</td></tr><tr><td></td><td>route-map map-name</td><td>(Optional) Specifies to advertise the default route if the route map is satisfied. The map-name argument can be any alphanumeric string up to 63 characters.</td></tr></table></div>	Syntax Description	always	(Optional) Specifies to always advertise the default route regardless of whether the route table has a default route.		route-map map-name	(Optional) Specifies to advertise the default route if the route map is satisfied. The map-name argument can be any alphanumeric string up to 63 characters.	<div>Examples</div> <div><ul style="list-style-type: none">These commands will always advertise the OSPFv3 default route regardless of whether the switch has a default route configured.<div>switch(config)#ipv6 router ospf 1</div><div>switch(config-router-ospf3)#default-information originate always</div><div>switch(config-router-ospf3)#show active</div><div>ipv6 router ospf 1</div><div>default-information originate always</div>These commands configures OSPF area 1 as metric of 100 for the default route with an external metric type of Type 1.<div>switch(config)#ipv6 router ospf 1</div><div>switch(config-router-ospf3)#default-information originate metric 100 metric-type 1</div><div>switch(config-router-ospf3)#show active</div><div>ipv6 router ospf 1</div><div>default-information originate metric 100 metric-type 1</div><div>switch(config-router-ospf3)#</div></div>
	Syntax Description	always	(Optional) Specifies to always advertise the default route regardless of whether the route table has a default route.					
		route-map map-name	(Optional) Specifies to advertise the default route if the route map is satisfied. The map-name argument can be any alphanumeric string up to 63 characters.					
	<div>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 5.x (2010), at L3-155.</div>	<div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1506.</div>						
		<div>See also Arista User Manual v. 4.12.3 (7/17/13), at 1291; Arista User Manual, v. 4.11.1 (1/11/13), at 1041.</div>						

Copyright Registration Information	Cisco	Arista						
<p>Cisco NX-OS 4.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>default-information originate (OSPFv3)</p> <p>To generate a default external route into an Open Shortest Path First version 3 (OSPFv3) routing domain, use the default-information originate command. To disable this feature, use the no form of this command.</p> <pre>default-information originate [always] [route-map map-name] no default-information originate [always] [route-map map-name]</pre> <table border="1"> <tr> <td>Syntax Description</td><td>always</td><td>(Optional) Specifies to always advertise the default route regardless of whether the route table has a default route.</td></tr> <tr> <td></td><td>route-map map-name</td><td>(Optional) Specifies to advertise the default route if the route map is satisfied. The map-name argument can be any alphanumeric string up to 63 characters.</td></tr> </table> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 4.x (2008), at L3-90.</p>	Syntax Description	always	(Optional) Specifies to always advertise the default route regardless of whether the route table has a default route.		route-map map-name	(Optional) Specifies to advertise the default route if the route map is satisfied. The map-name argument can be any alphanumeric string up to 63 characters.	<p>Examples</p> <ul style="list-style-type: none"> These commands will always advertise the OSPFv3 default route regardless of whether the switch has a default route configured. <pre>switch(config)#ipv6 router ospf 1 switch(config-router-ospf3)#default-information originate always switch(config-router-ospf3)#show active ipv6 router ospf 1 default-information originate always</pre> These commands configure OSPF area 1 as metric of 100 for the default route with an external metric type of Type 1. <pre>switch(config)#ipv6 router ospf 1 switch(config-router-ospf3)#default-information originate metric 100 metric-type 1 switch(config-router-ospf3)#show active ipv6 router ospf 1 default-information originate metric 100 metric-type 1 switch(config-router-ospf3)#</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1506.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1291; Arista User Manual, v. 4.11.1 (1/11/13), at 1041.</p>
Syntax Description	always	(Optional) Specifies to always advertise the default route regardless of whether the route table has a default route.						
	route-map map-name	(Optional) Specifies to advertise the default route if the route map is satisfied. The map-name argument can be any alphanumeric string up to 63 characters.						

Copyright Registration Information	Cisco	Arista				
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<p>distance (EIGRP)</p> <p>To allow the use of two administrative distances—internal and external—for the Enhanced Interior Gateway Routing Protocol (EIGRP) that could provide a better route to a node, use the distance command. To reset to default, use the no form of this command.</p> <p>distance <i>internal-distance external-distance</i></p> <p>no distance</p> <table><tr><td>Syntax Description</td><td><i>internal-distance</i> Administrative distance for EIGRP internal routes. Internal routes are routes that are learned from another entity within the same autonomous system (AS). The distance can be a value from 1 to 255. The default value is 90.</td></tr><tr><td></td><td><i>external-distance</i> Administrative distance for EIGRP external routes. External routes are routes for which the best path is learned from a source external to this autonomous system. The distance can be a value from 1 to 255. The default value is 170.</td></tr></table> <p>Defaults</p> <p><i>internal-distance:</i> 90 <i>external-distance:</i> 170</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference (2013), at 61.</p>	Syntax Description	<i>internal-distance</i> Administrative distance for EIGRP internal routes. Internal routes are routes that are learned from another entity within the same autonomous system (AS). The distance can be a value from 1 to 255. The default value is 90.		<i>external-distance</i> Administrative distance for EIGRP external routes. External routes are routes for which the best path is learned from a source external to this autonomous system. The distance can be a value from 1 to 255. The default value is 170.	<p>distance bgp</p> <p>The distance bgp command assigns an administrative distance to routes that the switch learns through BGP. Routers use administrative distances to select a route when two protocols provide routing information to the same destination. Distance values range from 1 to 255; lower distance values correspond to higher reliability. BGP routing tables do not include routes with a distance of 255.</p> <p>The distance command assigns distance values to external, internal, and local BGP routes:</p> <ul style="list-style-type: none">external: External routes are routes for which the best path is learned from a neighbor external to the autonomous system. Default distance is 200.internal: Internal routes are routes learned from a BGP entity within the same autonomous system. Default distance is 200.local: Local routes are networks listed with a network router configuration command for that router or for networks that are redistributed from another process. Default distance is 200. <p>The no distance bgp and default distance bgp commands restore the default administrative distances by removing the distance bgp command from <i>running-config</i>.</p> <p>Platform all Command Mode Router-BGP Configuration</p> <p>Command Syntax</p> <p>distance bgp <i>external_dist</i> [<i>INTERNAL_LOCAL</i>] no distance bgp default distance bgp</p> <p>Parameters</p> <ul style="list-style-type: none"><i>external_dist</i> distance assigned to external routes. Values range from 1 to 255.<i>INTERNAL_LOCAL</i> distance assigned to internal and local routes. Values for both routes range from 1 to 255. Options include:<ul style="list-style-type: none"><no parameter> <i>external_dist</i> value is assigned to internal and local routes.<i>internal_dist local_dist</i> values assigned to internal (<i>internal_dist</i>) and local (<i>local_dist</i>) routes. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1583.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1360; Arista User Manual, v. 4.11.1 (1/11/13), at 1106; Arista User Manual v. 4.10.3 (10/22/12), at 918; Arista User Manual v. 4.9.3.2 (5/3/12), at 684; Arista User Manual v. 4.8.2 (11/18/11), at 514; Arista User Manual v. 4.7.3 (7/18/11), at 379.</p>
	Syntax Description	<i>internal-distance</i> Administrative distance for EIGRP internal routes. Internal routes are routes that are learned from another entity within the same autonomous system (AS). The distance can be a value from 1 to 255. The default value is 90.				
	<i>external-distance</i> Administrative distance for EIGRP external routes. External routes are routes for which the best path is learned from a source external to this autonomous system. The distance can be a value from 1 to 255. The default value is 170.					

Copyright Registration Information	Cisco	Arista				
Cisco NX-OS 5.0 Effective date of registration: 11/13/2014	<p>distance (EIGRP)</p> <p>To allow the use of two administrative distances—internal and external—for the Enhanced Interior Gateway Routing Protocol (EIGRP) that could provide a better route to a node, use the distance command. To reset to default, use the no form of this command.</p> <p>distance <i>internal-distance external-distance</i></p> <p>no distance</p> <table><tr><td>Syntax Description</td><td><i>internal-distance</i> Administrative distance for EIGRP internal routes. Internal routes are routes that are learned from another entity within the same autonomous system (AS). The distance can be a value from 1 to 255. The default value is 90.</td></tr><tr><td></td><td><i>external-distance</i> Administrative distance for EIGRP external routes. External routes are routes for which the best path is learned from a source external to this autonomous system. The distance can be a value from 1 to 255. The default value is 170.</td></tr></table> <p>Defaults</p> <p><i>internal-distance</i>: 90 <i>external-distance</i>: 170</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 5.x (2010), at L3-171.</p>	Syntax Description	<i>internal-distance</i> Administrative distance for EIGRP internal routes. Internal routes are routes that are learned from another entity within the same autonomous system (AS). The distance can be a value from 1 to 255. The default value is 90.		<i>external-distance</i> Administrative distance for EIGRP external routes. External routes are routes for which the best path is learned from a source external to this autonomous system. The distance can be a value from 1 to 255. The default value is 170.	<p>distance bgp</p> <p>The distance bgp command assigns an administrative distance to routes that the switch learns through BGP. Routers use administrative distances to select a route when two protocols provide routing information to the same destination. Distance values range from 1 to 255; lower distance values correspond to higher reliability. BGP routing tables do not include routes with a distance of 255.</p> <p>The distance command assigns distance values to external, internal, and local BGP routes:</p> <ul style="list-style-type: none">external: External routes are routes for which the best path is learned from a neighbor external to the autonomous system. Default distance is 200.internal: Internal routes are routes learned from a BGP entity within the same autonomous system. Default distance is 200.local: Local routes are networks listed with a network router configuration command for that router or for networks that are redistributed from another process. Default distance is 200. <p>The no distance bgp and default distance bgp commands restore the default administrative distances by removing the distance bgp command from <i>running-config</i>.</p> <p>Platform all Command Mode Router-BGP Configuration</p> <p>Command Syntax</p> <p>distance bgp <i>external_dist</i> [<i>INTERNAL_LOCAL</i>] no distance bgp default distance bgp</p> <p>Parameters</p> <ul style="list-style-type: none"><i>external_dist</i> distance assigned to external routes. Values range from 1 to 255.<i>INTERNAL_LOCAL</i> distance assigned to internal and local routes. Values for both routes range from 1 to 255. Options include:<ul style="list-style-type: none"><no parameter> <i>external_dist</i> value is assigned to internal and local routes.<i>internal_dist local_dist</i> values assigned to internal (<i>internal_dist</i>) and local (<i>local_dist</i>) routes. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1583.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1360; Arista User Manual, v. 4.11.1 (1/11/13), at 1106; Arista User Manual v. 4.10.3 (10/22/12), at 918; Arista User Manual v. 4.9.3.2 (5/3/12), at 684; Arista User Manual v. 4.8.2 (11/18/11), at 514; Arista User Manual v. 4.7.3 (7/18/11), at 379.</p>
	Syntax Description	<i>internal-distance</i> Administrative distance for EIGRP internal routes. Internal routes are routes that are learned from another entity within the same autonomous system (AS). The distance can be a value from 1 to 255. The default value is 90.				
	<i>external-distance</i> Administrative distance for EIGRP external routes. External routes are routes for which the best path is learned from a source external to this autonomous system. The distance can be a value from 1 to 255. The default value is 170.					

Copyright Registration Information	Cisco	Arista				
Cisco NX-OS 4.0 Effective date of registration: 11/13/2014	<p>distance (EIGRP)</p> <p>To allow the use of two administrative distances—internal and external—for the Enhanced Interior Gateway Routing Protocol (EIGRP) that could provide a better route to a node, use the distance command. To reset to default, use the no form of this command.</p> <p>distance <i>internal-distance external-distance</i></p> <p>no distance</p> <table><tr><td>Syntax Description</td><td><i>internal-distance</i> Administrative distance for EIGRP internal routes. Internal routes are routes that are learned from another entity within the same autonomous system (AS). The distance can be a value from 1 to 255. The default value is 90.</td></tr><tr><td></td><td><i>external-distance</i> Administrative distance for EIGRP external routes. External routes are routes for which the best path is learned from a source external to this autonomous system. The distance can be a value from 1 to 255. The default value is 170.</td></tr></table> <p>Defaults</p> <p><i>internal-distance</i>: 90 <i>external-distance</i>: 170</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 4.x (2008), at L3-104.</p>	Syntax Description	<i>internal-distance</i> Administrative distance for EIGRP internal routes. Internal routes are routes that are learned from another entity within the same autonomous system (AS). The distance can be a value from 1 to 255. The default value is 90.		<i>external-distance</i> Administrative distance for EIGRP external routes. External routes are routes for which the best path is learned from a source external to this autonomous system. The distance can be a value from 1 to 255. The default value is 170.	<p>distance bgp</p> <p>The distance bgp command assigns an administrative distance to routes that the switch learns through BGP. Routers use administrative distances to select a route when two protocols provide routing information to the same destination. Distance values range from 1 to 255; lower distance values correspond to higher reliability. BGP routing tables do not include routes with a distance of 255.</p> <p>The distance command assigns distance values to external, internal, and local BGP routes:</p> <ul style="list-style-type: none">external: External routes are routes for which the best path is learned from a neighbor external to the autonomous system. Default distance is 200.internal: Internal routes are routes learned from a BGP entity within the same autonomous system. Default distance is 200.local: Local routes are networks listed with a network router configuration command for that router or for networks that are redistributed from another process. Default distance is 200. <p>The no distance bgp and default distance bgp commands restore the default administrative distances by removing the distance bgp command from <i>running-config</i>.</p> <p>Platform all Command Mode Router-BGP Configuration</p> <p>Command Syntax</p> <p>distance bgp <i>external_dist</i> [<i>INTERNAL_LOCAL</i>] no distance bgp default distance bgp</p> <p>Parameters</p> <ul style="list-style-type: none"><i>external_dist</i> distance assigned to external routes. Values range from 1 to 255.<i>INTERNAL_LOCAL</i> distance assigned to internal and local routes. Values for both routes range from 1 to 255. Options include:<ul style="list-style-type: none"><no parameter> <i>external_dist</i> value is assigned to internal and local routes.<i>internal_dist local_dist</i> values assigned to internal (<i>internal_dist</i>) and local (<i>local_dist</i>) routes. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1583.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1360; Arista User Manual, v. 4.11.1 (1/11/13), at 1106; Arista User Manual v. 4.10.3 (10/22/12), at 918; Arista User Manual v. 4.9.3.2 (5/3/12), at 684; Arista User Manual v. 4.8.2 (11/18/11), at 514; Arista User Manual v. 4.7.3 (7/18/11), at 379.</p>
	Syntax Description	<i>internal-distance</i> Administrative distance for EIGRP internal routes. Internal routes are routes that are learned from another entity within the same autonomous system (AS). The distance can be a value from 1 to 255. The default value is 90.				
	<i>external-distance</i> Administrative distance for EIGRP external routes. External routes are routes for which the best path is learned from a source external to this autonomous system. The distance can be a value from 1 to 255. The default value is 170.					

Copyright Registration Information	Cisco	Arista				
Cisco IOS 15.0 Effective date of registration: 11/28/2014	<p>distance (EIGRP)</p> <p>To allow the use of two administrative distances—internal and external—for the Enhanced Interior Gateway Routing Protocol (EIGRP) that could provide a better route to a node, use the distance command. To reset to default, use the no form of this command.</p> <p>distance <i>internal-distance external-distance</i></p> <p>no distance</p> <table><tr><td>Syntax Description</td><td><i>internal-distance</i> Administrative distance for EIGRP internal routes. Internal routes are routes that are learned from another entity within the same autonomous system (AS). The distance can be a value from 1 to 255. The default value is 90.</td></tr><tr><td></td><td><i>external-distance</i> Administrative distance for EIGRP external routes. External routes are routes for which the best path is learned from a source external to this autonomous system. The distance can be a value from 1 to 255. The default value is 170.</td></tr></table> <p>Defaults</p> <p><i>internal-distance:</i> 90 <i>external-distance:</i> 170</p> <p>Cisco IOS IP Routing: EIGRP Command Reference (2009), at IRE-33.</p>	Syntax Description	<i>internal-distance</i> Administrative distance for EIGRP internal routes. Internal routes are routes that are learned from another entity within the same autonomous system (AS). The distance can be a value from 1 to 255. The default value is 90.		<i>external-distance</i> Administrative distance for EIGRP external routes. External routes are routes for which the best path is learned from a source external to this autonomous system. The distance can be a value from 1 to 255. The default value is 170.	<p>distance bgp</p> <p>The distance bgp command assigns an administrative distance to routes that the switch learns through BGP. Routers use administrative distances to select a route when two protocols provide routing information to the same destination. Distance values range from 1 to 255; lower distance values correspond to higher reliability. BGP routing tables do not include routes with a distance of 255.</p> <p>The distance command assigns distance values to external, internal, and local BGP routes:</p> <ul style="list-style-type: none">external: External routes are routes for which the best path is learned from a neighbor external to the autonomous system. Default distance is 200.internal: Internal routes are routes learned from a BGP entity within the same autonomous system. Default distance is 200.local: Local routes are networks listed with a network router configuration command for that router or for networks that are redistributed from another process. Default distance is 200. <p>The no distance bgp and default distance bgp commands restore the default administrative distances by removing the distance bgp command from <i>running-config</i>.</p> <p>Platform all Command Mode Router-BGP Configuration</p> <p>Command Syntax</p> <p>distance bgp <i>external_dist</i> [<i>INTERNAL_LOCAL</i>] no distance bgp default distance bgp</p> <p>Parameters</p> <ul style="list-style-type: none"><i>external_dist</i> distance assigned to external routes. Values range from 1 to 255.<i>INTERNAL_LOCAL</i> distance assigned to internal and local routes. Values for both routes range from 1 to 255. Options include:<ul style="list-style-type: none"><no parameter> <i>external_dist</i> value is assigned to internal and local routes.<i>internal_dist local_dist</i> values assigned to internal (<i>internal_dist</i>) and local (<i>local_dist</i>) routes. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1583.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1360; Arista User Manual, v. 4.11.1 (1/11/13), at 1106; Arista User Manual v. 4.10.3 (10/22/12), at 918; Arista User Manual v. 4.9.3.2 (5/3/12), at 684; Arista User Manual v. 4.8.2 (11/18/11), at 514; Arista User Manual v. 4.7.3 (7/18/11), at 379.</p>
	Syntax Description	<i>internal-distance</i> Administrative distance for EIGRP internal routes. Internal routes are routes that are learned from another entity within the same autonomous system (AS). The distance can be a value from 1 to 255. The default value is 90.				
	<i>external-distance</i> Administrative distance for EIGRP external routes. External routes are routes for which the best path is learned from a source external to this autonomous system. The distance can be a value from 1 to 255. The default value is 170.					

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>When you configure the <code>ip</code> command on an interface, the handling of proxy Address Resolution Protocol (ARP) requests changes (unless proxy ARP was disabled). Hosts send ARP requests to <u>map an IP address to a MAC address</u>. The GLBP gateway intercepts the ARP requests and replies to the ARP requests on behalf of the connected nodes. If a forwarder in the GLBP group is active, proxy ARP requests are answered using the MAC address of the first active forwarder in the group. If no forwarder is active, proxy ARP responses are suppressed.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference (2013), at 256.</p>	<p>Displaying ARP Entries</p> <p>The <code>show ip arp</code> command displays ARP cache entries that <u>map an IP address to a corresponding MAC address</u>. The table displays addresses by their host names when the command includes the <code>resolve</code> argument.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1225.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1038; Arista User Manual, v. 4.11.1 (1/11/13), at 840; Arista User Manual v. 4.10.3 (10/22/12), at 687.</p>
<p>Cisco NX-OS 5.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>When you configure the <code>ip</code> command on an interface, the handling of proxy Address Resolution Protocol (ARP) requests changes (unless proxy ARP was disabled). Hosts send ARP requests to <u>map an IP address to a MAC address</u>. The GLBP gateway intercepts the ARP requests and replies to the ARP requests on behalf of the connected nodes. If a forwarder in the GLBP group is active, proxy ARP requests are answered using the MAC address of the first active forwarder in the group. If no forwarder is active, proxy ARP responses are suppressed.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 5.x (2010), at L3-236.</p>	<p>Displaying ARP Entries</p> <p>The <code>show ip arp</code> command displays ARP cache entries that <u>map an IP address to a corresponding MAC address</u>. The table displays addresses by their host names when the command includes the <code>resolve</code> argument.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1225.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1038; Arista User Manual, v. 4.11.1 (1/11/13), at 840; Arista User Manual v. 4.10.3 (10/22/12), at 687.</p>
<p>Cisco NX-OS 4.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>When you configure the <code>ip</code> command on an interface, the handling of proxy Address Resolution Protocol (ARP) requests changes (unless proxy ARP was disabled). Hosts send ARP requests to <u>map an IP address to a MAC address</u>. The GLBP gateway intercepts the ARP requests and replies to the ARP requests on behalf of the connected nodes. If a forwarder in the GLBP group is active, proxy ARP requests are answered using the MAC address of the first active forwarder in the group. If no forwarder is active, proxy ARP responses are suppressed.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 4.x (2008), at L3-143.</p>	<p>Displaying ARP Entries</p> <p>The <code>show ip arp</code> command displays ARP cache entries that <u>map an IP address to a corresponding MAC address</u>. The table displays addresses by their host names when the command includes the <code>resolve</code> argument.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1225.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1038; Arista User Manual, v. 4.11.1 (1/11/13), at 840; Arista User Manual v. 4.10.3 (10/22/12), at 687.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 15.0</p> <p>Effective date of registration: 11/28/2014</p>	<p>Address Resolution Protocol (ARP) is an Internet protocol used to map an IP address to a MAC address. ARP finds the MAC address, also known as the hardware address, of an IP-routed host from its known IP address and maintains this mapping information in a table. The router uses this IP address and MAC address mapping information to send IP packets to the next-hop router in the network.</p> <p>Cisco IOS IP Addressing Services Configuration Guide (2009), at CSI-CLI-00061623.</p>	<p>Displaying ARP Entries</p> <p>The <code>show ip arp</code> command displays ARP cache entries that map an IP address to a corresponding MAC address. The table displays addresses by their host names when the command includes the <code>resolve</code> argument.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1225.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1038; Arista User Manual, v. 4.11.1 (1/11/13), at 840; Arista User Manual v. 4.10.3 (10/22/12), at 687.</p>
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>Expanded Community Lists</p> <p>Expanded community lists are used to filter communities using a regular expression. Regular expressions are used to configure patterns to match community attributes. The order for matching using the * or + character is longest construct first. Nested constructs are matched from the outside in. Concatenated constructs are matched beginning at the left side. If a regular expression can match two different parts of an input string, it will match the earliest part first.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference (2013), at 274.</p>	<p>The order for matching using the * or + character is longest construct first. Nested constructs are matched from the outside in. Concatenated constructs are matched beginning at the left side. If a regular expression can match two different parts of an input string, it matches the earliest part first.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 107.</p> <p><i>See also</i> Arista User Manual v. 4.13.6F (4/14/2014), at 105; Arista User Manual, v. 4.11.1 (1/11/13), at 65; Arista User Manual v. 4.12.3 (7/17/13), at 95; Arista User Manual v. 4.10.3 (10/22/12), at 57; Arista User Manual v. 4.9.3.2 (5/3/12), at 53; Arista User Manual v. 4.8.2 (11/18/11), at 49.</p>
<p>Cisco IOS 15.0</p> <p>Effective date of registration: 11/28/2014</p>	<p>Expanded Community Lists</p> <p>Expanded community lists are used to filter communities using a regular expression. Regular expressions are used to configure patterns to match community attributes. The order for matching using the * or + character is longest construct first. Nested constructs are matched from the outside in. Concatenated constructs are matched beginning at the left side. If a regular expression can match two different parts of an input string, it will match the earliest part first.</p> <p>Cisco IOS IP Routing: BGP Command Reference, (2009), at 274.</p>	<p>The order for matching using the * or + character is longest construct first. Nested constructs are matched from the outside in. Concatenated constructs are matched beginning at the left side. If a regular expression can match two different parts of an input string, it matches the earliest part first.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 107.</p> <p><i>See also</i> Arista User Manual v. 4.13.6F (4/14/2014), at 105; Arista User Manual, v. 4.11.1 (1/11/13), at 65; Arista User Manual v. 4.12.3 (7/17/13), at 95; Arista User Manual v. 4.10.3 (10/22/12), at 57; Arista User Manual v. 4.9.3.2 (5/3/12), at 53; Arista User Manual v. 4.8.2 (11/18/11), at 49.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>Static routes have a default administrative distance of 1. If you want a dynamic routing protocol to take precedence over a static route, you must configure the static route preference argument to be greater than the administrative distance of the dynamic routing protocol. For example, routes derived with Enhanced Interior Gateway Routing Protocol (EIGRP) have a default administrative distance of 100. To have a static route that would be overridden by an EIGRP dynamic route, specify an administrative distance greater than 100.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference (2013), at 337.</p>	<p>Static routes have a default administrative distance of 1. Assigning a higher administrative distance to a static route configures it to be overridden by dynamic routing data. For example, a static route with a distance value of 200 is overridden by OSPF intra-area routes with a default distance of 110.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2/2014), at 1226.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1082; Arista User Manual, v. 4.11.1 (1/11/13), at 860; Arista User Manual v. 4.10.3 (10/22/12), at 683.</p>
<p>Cisco NX-OS 5.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>Static routes have a default administrative distance of 1. If you want a dynamic routing protocol to take precedence over a static route, you must configure the static route preference argument to be greater than the administrative distance of the dynamic routing protocol. For example, routes derived with Enhanced Interior Gateway Routing Protocol (EIGRP) have a default administrative distance of 100. To have a static route that would be overridden by an EIGRP dynamic route, specify an administrative distance greater than 100.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 5.x (2010), at L3-311.</p>	<p>Static routes have a default administrative distance of 1. Assigning a higher administrative distance to a static route configures it to be overridden by dynamic routing data. For example, a static route with a distance value of 200 is overridden by OSPF intra-area routes with a default distance of 110.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2/2014), at 1226.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1082; Arista User Manual, v. 4.11.1 (1/11/13), at 860; Arista User Manual v. 4.10.3 (10/22/12), at 683.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>is-type</p> <p>To configure the routing level for an instance of the Intermediate System-to-Intermediate System (IS-IS) routing process, use the is-type command. To reset the default value, use the no form of this command.</p> <p>is-type {level-1 level-1-2 level-2}</p> <p>no is-type {level-1 level-1-2 level-2}</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference (2013), at 407.</p>	<p>is-type</p> <p>The is-type command configures the routing level for an instance of the IS-IS routing instance.</p> <p>Platform all Command Mode Router-IS-IS Configuration</p> <p>Command Syntax is-type LAYER_VALUE</p> <p>Parameters</p> <ul style="list-style-type: none"> LAYER_VALUE layer value. Options include: <ul style="list-style-type: none"> level-1 The switch operates as a Level-1 (intra-area) router. level-2 The switch operates as a Level-2 (inter-area) router. <p>Example</p> <ul style="list-style-type: none"> These commands configure Level 2 routing on interface Ethernet 5. <pre>switch(config)#router isis Osiris switch(config-router-isis)#is-type level-2 switch(config-router-isis)#</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1691.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1451.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 5.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>is-type</p> <p>To configure the routing level for an instance of the Intermediate System-to-Intermediate System (IS-IS) routing process, use the is-type command. To reset the default value, use the no form of this command.</p> <pre>is-type {level-1 level-1-2 level-2} no is-type {level-1 level-1-2 level-2}</pre> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 5.x (2010), at L3-373.</p>	<p>is-type</p> <p>The is-type command configures the routing level for an instance of the IS-IS routing instance.</p> <p>Platform all Command Mode Router-IS-IS Configuration</p> <p>Command Syntax is-type <i>LAYER_VALUE</i></p> <p>Parameters</p> <ul style="list-style-type: none"> <i>LAYER_VALUE</i> layer value. Options include: <ul style="list-style-type: none"> — level-1 The switch operates as a Level-1 (intra-area) router. — level-2 The switch operates as a Level-2 (inter-area) router. <p>Example</p> <ul style="list-style-type: none"> These commands configure Level 2 routing on interface Ethernet 5. <pre>switch(config)#router isis Osiris switch(config-router-isis)#is-type level-2 switch(config-router-isis)#</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1691.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1451.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 4.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>is-type</p> <p>To configure the routing level for an instance of the Intermediate System-to-Intermediate System (IS-IS) routing process, use the is-type command. To reset the default value, use the no form of this command.</p> <pre>is-type {level-1 level-1-2 level-2} no is-type {level-1 level-1-2 level-2}</pre> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 4.x (2008), at L3-208.</p>	<p>is-type</p> <p>The is-type command configures the routing level for an instance of the IS-IS routing instance.</p> <p>Platform all Command Mode Router-IS-IS Configuration</p> <p>Command Syntax is-type <i>LAYER_VALUE</i></p> <p>Parameters</p> <ul style="list-style-type: none"> <i>LAYER_VALUE</i> layer value. Options include: <ul style="list-style-type: none"> — level-1 The switch operates as a Level-1 (intra-area) router. — level-2 The switch operates as a Level-2 (inter-area) router. <p>Example</p> <ul style="list-style-type: none"> These commands configure Level 2 routing on interface Ethernet 5. <pre>switch(config)#router isis Osiris switch(config-router-isis)#is-type level-2 switch(config-router-isis)#</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1691.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1451.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 15.0</p> <p>Effective date of registration: 11/28/2014</p>	<p>is-type</p> <p>To configure the routing level for an instance of the Intermediate System-to-Intermediate System (IS-IS) routing process, use the is-type command in router configuration mode. To reset the default value, use the no form of this command.</p> <p>is-type [level-1 level-1-2 level-2 only] no is-type [level-1 level-1-2 level-2-only]</p> <p>Cisco IOS IP Routing: ISIS Command Reference (2009), at IRS-73.</p>	<p>is-type</p> <p>The is-type command configures the routing level for an instance of the IS-IS routing instance.</p> <p>Platform all Command Mode Router-IS-IS Configuration</p> <p>Command Syntax is-type LAYER_VALUE</p> <p>Parameters</p> <ul style="list-style-type: none"> LAYER_VALUE layer value. Options include: <ul style="list-style-type: none"> — level-1 The switch operates as a Level-1 (intra-area) router. — level-2 The switch operates as a Level-2 (inter-area) router. <p>Example</p> <ul style="list-style-type: none"> These commands configure Level 2 routing on interface Ethernet 5. <pre>switch(config)#router isis Osiris switch(config-router-isis)#is-type level-2 switch(config-router-isis)#</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1691.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1451.</p>

Copyright Registration Information	Cisco	Arista													
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<p>isis hello-multiplier</p> <p>To specify the number of Intermediate System-to-Intermediate System (IS-IS) hello packets a neighbor must miss before the router should declare the adjacency as down, use the isis hello-multiplier command. To restore the default value, use the no form of this command.</p> <p>isis hello-multiplier multiplier [level-1 level-2]</p> <p>no isis hello-multiplier [level-1 level-2]</p> <table><tr><td>Syntax Description</td><td><i>multiplier</i></td><td>Integer value. Range: 3 to 1000. Default: 3.</td></tr><tr><td></td><td>level-1</td><td>Configures the hello multiplier independently for Level 1 adjacencies.</td></tr><tr><td></td><td>level-2</td><td>Configures the hello multiplier independently for Level 2 adjacencies.</td></tr></table> <p>Command Default The default settings are as follows:</p> <ul style="list-style-type: none">• <i>multiplier</i>: 3• Level 1 and Level 2 <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference (2013), at 423.</p>	Syntax Description	<i>multiplier</i>	Integer value. Range: 3 to 1000. Default: 3.		level-1	Configures the hello multiplier independently for Level 1 adjacencies.		level-2	Configures the hello multiplier independently for Level 2 adjacencies.	<p>isis hello-multiplier</p> <p>The isis hello-multiplier command specifies the number of IS-IS hello packets a neighbor must miss before the device should declare the adjacency as down.</p> <p>Each hello packet contains a hold time. The hold time informs the receiving devices how long to wait without seeing another hello from the sending device before considering the sending device down. The isis hello-multiplier command is used to calculate the hold time announced in hello packets by multiplying this number with the configured isis hello-interval.</p> <p>The no isis hello-multiplier and default isis hello-multiplier commands restore the default hello interval of 3 on the configuration mode interface by removing the isis hello-multiplier command from <i>running-config</i>.</p> <table><tr><td>Platform</td><td>all</td></tr><tr><td>Command Mode</td><td>Interface-Ethernet Configuration Interface-Loopback Configuration Interface-Port-channel Configuration Interface-VLAN Configuration</td></tr></table> <p>Command Syntax</p> <p>isis hello-multiplier factor</p> <p>no isis hello-multiplier</p> <p>default isis hello-multiplier</p> <p>Parameters</p> <ul style="list-style-type: none">• <i>factor</i> hello multiplier. Values range from 3 to 100; default is 3. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1685.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1447.</p>	Platform	all	Command Mode	Interface-Ethernet Configuration Interface-Loopback Configuration Interface-Port-channel Configuration Interface-VLAN Configuration
	Syntax Description	<i>multiplier</i>	Integer value. Range: 3 to 1000. Default: 3.												
		level-1	Configures the hello multiplier independently for Level 1 adjacencies.												
	level-2	Configures the hello multiplier independently for Level 2 adjacencies.													
Platform	all														
Command Mode	Interface-Ethernet Configuration Interface-Loopback Configuration Interface-Port-channel Configuration Interface-VLAN Configuration														

Copyright Registration Information	Cisco	Arista																	
Cisco NX-OS 5.0 Effective date of registration: 11/13/2014	<div>isis hello-multiplier</div> <div>To specify the number of Intermediate System-to-Intermediate System (IS-IS) hello packets a neighbor must miss before the router should declare the adjacency as down, use the isis hello-multiplier command. To restore the default value, use the no form of this command.</div> <div>isis hello-multiplier multiplier {level-1 level-2}</div> <div>no isis hello-multiplier {level-1 level-2}</div> <div><table><tr><td>Syntax Description</td><td>multiplier</td><td>Integer value. Range: 3 to 1000. Default: 3.</td></tr><tr><td></td><td>level-1</td><td>Configures the hello multiplier independently for Level 1 adjacencies.</td></tr><tr><td></td><td>level-2</td><td>Configures the hello multiplier independently for Level 2 adjacencies.</td></tr></table></div> <div><table><tr><td>Command Default</td><td>The default settings are as follows:</td></tr><tr><td></td><td><ul style="list-style-type: none">multiplier: 3Level 1 and Level 2</td></tr></table></div> <div>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 5.x (2010), at L3-389.</div>	Syntax Description	multiplier	Integer value. Range: 3 to 1000. Default: 3.		level-1	Configures the hello multiplier independently for Level 1 adjacencies.		level-2	Configures the hello multiplier independently for Level 2 adjacencies.	Command Default	The default settings are as follows:		<ul style="list-style-type: none">multiplier: 3Level 1 and Level 2	<div>isis hello-multiplier</div> <div>The isis hello-multiplier command specifies the number of IS-IS hello packets a neighbor must miss before the device should declare the adjacency as down.</div> <div>Each hello packet contains a hold time. The hold time informs the receiving devices how long to wait without seeing another hello from the sending device before considering the sending device down. The isis hello-multiplier command is used to calculate the hold time announced in hello packets by multiplying this number with the configured isis hello-interval.</div> <div>The no isis hello-multiplier and default isis hello-multiplier commands restore the default hello interval of 3 on the configuration mode interface by removing the isis hello-multiplier command from running-config.</div> <div><table><tr><td>Platform</td><td>all</td></tr><tr><td>Command Mode</td><td>Interface-Ethernet Configuration Interface-Loopback Configuration Interface-Port-channel Configuration Interface-VLAN Configuration</td></tr></table></div> <div>Comunand Syntax</div> <div>isis hello-multiplier factor</div> <div>no isis hello-multiplier</div> <div>default isis hello-multiplier</div> <div>Parameters</div> <div><ul style="list-style-type: none">factor hello multiplier. Values range from 3 to 100; default is 3.</div> <div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1685.</div> <div>See also Arista User Manual v. 4.12.3 (7/17/13), at 1447.</div>	Platform	all	Command Mode	Interface-Ethernet Configuration Interface-Loopback Configuration Interface-Port-channel Configuration Interface-VLAN Configuration
	Syntax Description	multiplier	Integer value. Range: 3 to 1000. Default: 3.																
		level-1	Configures the hello multiplier independently for Level 1 adjacencies.																
	level-2	Configures the hello multiplier independently for Level 2 adjacencies.																	
Command Default	The default settings are as follows:																		
	<ul style="list-style-type: none">multiplier: 3Level 1 and Level 2																		
Platform	all																		
Command Mode	Interface-Ethernet Configuration Interface-Loopback Configuration Interface-Port-channel Configuration Interface-VLAN Configuration																		

Copyright Registration Information	Cisco	Arista													
Cisco NX-OS 4.0 Effective date of registration: 11/13/2014	<div>isis hello-multiplier</div> <p>To specify the number of Intermediate System-to-Intermediate System (IS-IS) hello packets a neighbor must miss before the router should declare the adjacency as down, use the isis hello-multiplier command. To restore the default value, use the no form of this command.</p> <div>isis hello-multiplier multiplier [level-1 level-2]</div> <div>no isis hello-multiplier [level-1 level-2]</div> <table><tr><td>Syntax Description</td><td>multiplier</td><td>Integer value. Range: 3 to 1000. Default: 3.</td></tr><tr><td></td><td>level-1</td><td>Configures the hello multiplier independently for Level 1 adjacencies.</td></tr><tr><td></td><td>level-2</td><td>Configures the hello multiplier independently for Level 2 adjacencies.</td></tr></table> <div>Command Default</div> <p>The default settings are as follows:</p> <ul style="list-style-type: none">• multiplier: 3• Level 1 and Level 2 <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference (2008), at L3-224.</p>	Syntax Description	multiplier	Integer value. Range: 3 to 1000. Default: 3.		level-1	Configures the hello multiplier independently for Level 1 adjacencies.		level-2	Configures the hello multiplier independently for Level 2 adjacencies.	<div>isis hello-multiplier</div> <p>The isis hello-multiplier command specifies the number of IS-IS hello packets a neighbor must miss before the device should declare the adjacency as down.</p> <p>Each hello packet contains a hold time. The hold time informs the receiving devices how long to wait without seeing another hello from the sending device before considering the sending device down. The isis hello-multiplier command is used to calculate the hold time announced in hello packets by multiplying this number with the configured isis hello-interval.</p> <p>The no isis hello-multiplier and default isis hello-multiplier commands restore the default hello interval of 3 on the configuration mode interface by removing the isis hello-multiplier command from running-config.</p> <table><tr><td>Platform</td><td>all</td></tr><tr><td>Command Mode</td><td>Interface-Ethernet Configuration Interface-Loopback Configuration Interface-Port-channel Configuration Interface-VLAN Configuration</td></tr></table> <div>Command Syntax</div> <div>isis hello-multiplier factor</div> <div>no isis hello-multiplier</div> <div>default isis hello-multiplier</div> <div>Parameters</div> <ul style="list-style-type: none">• factor hello multiplier. Values range from 3 to 100; default is 3 <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1685.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1447.</p>	Platform	all	Command Mode	Interface-Ethernet Configuration Interface-Loopback Configuration Interface-Port-channel Configuration Interface-VLAN Configuration
	Syntax Description	multiplier	Integer value. Range: 3 to 1000. Default: 3.												
	level-1	Configures the hello multiplier independently for Level 1 adjacencies.													
	level-2	Configures the hello multiplier independently for Level 2 adjacencies.													
Platform	all														
Command Mode	Interface-Ethernet Configuration Interface-Loopback Configuration Interface-Port-channel Configuration Interface-VLAN Configuration														

Copyright Registration Information	Cisco	Arista													
Cisco IOS 15.0 Effective date of registration: 11/28/2014	<div>isis hello-multiplier</div> <p>To specify the number of Intermediate System-to-Intermediate System (IS-IS) hello packets a neighbor must miss before the router should declare the adjacency as down, use the isis hello-multiplier command. To restore the default value, use the no form of this command.</p> <div>isis hello-multiplier multiplier {level-1 level-2}</div> <div>no isis hello-multiplier {level-1 level-2}</div> <table><tr><td>Syntax Description</td><td>multiplier</td><td>Integer value. Range: 3 to 1000. Default: 3.</td></tr><tr><td></td><td>level-1</td><td>Configures the hello multiplier independently for Level 1 adjacencies.</td></tr><tr><td></td><td>level-2</td><td>Configures the hello multiplier independently for Level 2 adjacencies.</td></tr></table> <div>Command Default</div> <p>The default settings are as follows:</p> <ul style="list-style-type: none">multiplier: 3Level 1 and Level 2 <p>Cisco IOS IP Routing: ISIS Command Reference (2009), at IRS-54.</p>	Syntax Description	multiplier	Integer value. Range: 3 to 1000. Default: 3.		level-1	Configures the hello multiplier independently for Level 1 adjacencies.		level-2	Configures the hello multiplier independently for Level 2 adjacencies.	<div>isis hello-multiplier</div> <p>The isis hello-multiplier command specifies the number of IS-IS hello packets a neighbor must miss before the device should declare the adjacency as down.</p> <p>Each hello packet contains a hold time. The hold time informs the receiving devices how long to wait without seeing another hello from the sending device before considering the sending device down. The isis hello-multiplier command is used to calculate the hold time announced in hello packets by multiplying this number with the configured isis hello-interval.</p> <p>The no isis hello-multiplier and default isis hello-multiplier commands restore the default hello interval of 3 on the configuration mode interface by removing the isis hello-multiplier command from running-config.</p> <table><tr><td>Platform</td><td>all</td></tr><tr><td>Command Mode</td><td>Interface-Ethernet Configuration Interface-Loopback Configuration Interface-Port-channel Configuration Interface-VLAN Configuration</td></tr></table> <div>Command Syntax</div> <div>isis hello-multiplier factor</div> <div>no isis hello-multiplier</div> <div>default isis hello-multiplier</div> <div>Parameters</div> <ul style="list-style-type: none">factor hello multiplier. Values range from 3 to 100; default is 3. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1685.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1447.</p>	Platform	all	Command Mode	Interface-Ethernet Configuration Interface-Loopback Configuration Interface-Port-channel Configuration Interface-VLAN Configuration
	Syntax Description	multiplier	Integer value. Range: 3 to 1000. Default: 3.												
		level-1	Configures the hello multiplier independently for Level 1 adjacencies.												
	level-2	Configures the hello multiplier independently for Level 2 adjacencies.													
Platform	all														
Command Mode	Interface-Ethernet Configuration Interface-Loopback Configuration Interface-Port-channel Configuration Interface-VLAN Configuration														

Copyright Registration Information	Cisco	Arista															
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>isis priority</p> <p>To configure the priority of designated routers, use the isis priority command in interface configuration mode. To reset the default priority, use the no form of this command.</p> <p>isis priority <i>number-value</i> [<i>level-1</i> <i>level-2</i>]</p> <p>no isis priority [<i>level-1</i> <i>level-2</i>]</p> <table border="1"> <tr> <td>Syntax Description</td><td><i>number-value</i></td><td>Priority of a router and is a number from 0 to 127. The default value is 64.</td></tr> <tr> <td></td><td><i>level-1</i></td><td>(Optional) Sets the priority for Level 1 independently.</td></tr> <tr> <td></td><td><i>level-2</i></td><td>(Optional) Sets the priority for Level 2 independently.</td></tr> </table> <p>Defaults</p> <p>Priority of 64 Level 1 and Level 2</p> <p>Command Modes</p> <p>Interface configuration</p> <p>Supported User Roles</p> <p>network-admin vdc-admin</p> <table border="1"> <tr> <td>Command History</td><td>Release</td><td>Modification</td></tr> <tr> <td></td><td>4.0(1)</td><td>This command was introduced.</td></tr> </table> <p>Usage Guidelines</p> <p>Priorities can be configured for Level 1 and Level 2 independently. Specifying the <i>level-1</i> or <i>level-2</i> keyword resets priority only for Level 1 or Level 2 routing, respectively.</p> <p>The priority is used to determine which router on a LAN will be the designated router or Designated Intermediate System (DIS). The priorities are advertised in the hello packets. The router with the highest priority will become the DIS.</p> <p>In Intermediate System-to-Intermediate System (IS-IS), there is no backup designated router. Setting the priority to 0 lowers the chance of this system becoming the DIS, but does not prevent it. If a router with a higher priority comes on line, it will take over the role from the current DIS. In the case of equal priorities, the highest MAC address breaks the tie.</p> <p>This command requires the Enterprise Services license.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference (2013), at 433.</p>	Syntax Description	<i>number-value</i>	Priority of a router and is a number from 0 to 127. The default value is 64.		<i>level-1</i>	(Optional) Sets the priority for Level 1 independently.		<i>level-2</i>	(Optional) Sets the priority for Level 2 independently.	Command History	Release	Modification		4.0(1)	This command was introduced.	<p>isis priority</p> <p>The isis priority command configures IS-IS router priority for the configuration mode interface.</p> <p>The priority is used to determine which device will be the Designated Intermediate System (DIS). The device with the highest priority will become the DIS.</p> <p>In IS-IS, there is no backup designated router. Setting the priority to 0 lowers the chance of this system becoming the DIS, but does not prevent it. If a device with a higher priority comes on line, it will take over the role from the current DIS.</p> <p>The no isis priority and default isis priority commands restore the default priority (64) on the configuration mode interface.</p> <p>Platform all</p> <p>Command Mode Interface-Ethernet Configuration Interface-Loopback Configuration Interface-Port-channel Configuration Interface-VLAN Configuration</p> <p>Command Syntax</p> <p>isis priority <i>priority_level</i></p> <p>no isis priority</p> <p>default isis priority</p> <p>Parameters</p> <ul style="list-style-type: none"> <i>priority_level</i> priority level. Value ranges from 0 to 127. Default value is 64. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1690.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1450.</p>
Syntax Description	<i>number-value</i>	Priority of a router and is a number from 0 to 127. The default value is 64.															
	<i>level-1</i>	(Optional) Sets the priority for Level 1 independently.															
	<i>level-2</i>	(Optional) Sets the priority for Level 2 independently.															
Command History	Release	Modification															
	4.0(1)	This command was introduced.															

Copyright Registration Information	Cisco	Arista															
<p>Cisco NX-OS 5.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>isis priority</p> <p>To configure the priority of designated routers, use the isis priority command in interface configuration mode. To reset the default priority, use the no form of this command.</p> <p>isis priority <i>number-value</i> [level-1 level-2]</p> <p>no isis priority [level-1 level-2]</p> <table border="1"> <tr> <td>Syntax Description</td><td><i>number-value</i></td><td>Priority of a router and is a number from 0 to 127. The default value is 64.</td></tr> <tr> <td></td><td>level-1</td><td>(Optional) Sets the priority for Level 1 independently.</td></tr> <tr> <td></td><td>level-2</td><td>(Optional) Sets the priority for Level 2 independently.</td></tr> </table> <p>Defaults</p> <p>Priority of 64 Level 1 and Level 2</p> <p>Command Modes</p> <p>Interface configuration</p> <p>Supported User Roles</p> <p>network-admin vdc-admin</p> <table border="1"> <tr> <td>Command History</td><td>Release</td><td>Modification</td></tr> <tr> <td></td><td>4.0(1)</td><td>This command was introduced.</td></tr> </table> <p>Usage Guidelines</p> <p>Priorities can be configured for Level 1 and Level 2 independently. Specifying the level-1 or level-2 keyword resets priority only for Level 1 or Level 2 routing, respectively.</p> <p>The priority is used to determine which router on a LAN will be the designated router or Designated Intermediate System (DIS). The priorities are advertised in the hello packets. The router with the highest priority will become the DIS.</p> <p>In Intermediate System-to-Intermediate System (IS-IS), there is no backup designated router. Setting the priority to 0 lowers the chance of this system becoming the DIS, but does not prevent it. If a router with a higher priority comes on line, it will take over the role from the current DIS. In the case of equal priorities, the highest MAC address breaks the tie.</p> <p>This command requires the Enterprise Services license.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 5.x (2010), at L3-397.</p>	Syntax Description	<i>number-value</i>	Priority of a router and is a number from 0 to 127. The default value is 64.		level-1	(Optional) Sets the priority for Level 1 independently.		level-2	(Optional) Sets the priority for Level 2 independently.	Command History	Release	Modification		4.0(1)	This command was introduced.	<p>isis priority</p> <p>The isis priority command configures IS-IS router priority for the configuration mode interface.</p> <p>The priority is used to determine which device will be the Designated Intermediate System (DIS). The device with the highest priority will become the DIS.</p> <p>In IS-IS, there is no backup designated router. Setting the priority to 0 lowers the chance of this system becoming the DIS, but does not prevent it. If a device with a higher priority comes on line, it will take over the role from the current DIS.</p> <p>The no isis priority and default isis priority commands restore the default priority (64) on the configuration mode interface.</p> <p>Platform all</p> <p>Command Mode Interface-Ethernet Configuration Interface-Loopback Configuration Interface-Port-channel Configuration Interface-VLAN Configuration</p> <p>Command Syntax</p> <p>isis priority <i>priority_level</i></p> <p>no isis priority</p> <p>default isis priority</p> <p>Parameters</p> <ul style="list-style-type: none"> <i>priority_level</i> priority level. Value ranges from 0 to 127. Default value is 64. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1690.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1450.</p>
Syntax Description	<i>number-value</i>	Priority of a router and is a number from 0 to 127. The default value is 64.															
	level-1	(Optional) Sets the priority for Level 1 independently.															
	level-2	(Optional) Sets the priority for Level 2 independently.															
Command History	Release	Modification															
	4.0(1)	This command was introduced.															

Copyright Registration Information	Cisco	Arista															
<p>Cisco NX-OS 4.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>isis priority</p> <p>To configure the priority of designated routers, use the isis priority command in interface configuration mode. To reset the default priority, use the no form of this command.</p> <p>isis priority <i>number-value</i> [level-1 level-2]</p> <p>no isis priority [level-1 level-2]</p> <table border="1"> <tr> <td>Syntax Description</td><td><i>number-value</i></td><td>Priority of a router and is a number from 0 to 127. The default value is 64.</td></tr> <tr> <td></td><td>level-1</td><td>(Optional) Sets the priority for Level 1 independently.</td></tr> <tr> <td></td><td>level-2</td><td>(Optional) Sets the priority for Level 2 independently.</td></tr> </table> <p>Defaults</p> <p>Priority of 64 Level 1 and Level 2</p> <p>Command Modes</p> <p>Interface configuration</p> <p>Supported User Roles</p> <p>network-admin vdc-admin</p> <table border="1"> <tr> <td>Command History</td><td>Release</td><td>Modification</td></tr> <tr> <td></td><td>4.0(1)</td><td>This command was introduced.</td></tr> </table> <p>Usage Guidelines</p> <p>Priorities can be configured for Level 1 and Level 2 independently. Specifying the level-1 or level-2 keyword resets priority only for Level 1 or Level 2 routing, respectively.</p> <p>The priority is used to determine which router on a LAN will be the designated router or Designated Intermediate System (DIS). The priorities are advertised in the hello packets. The router with the highest priority will become the DIS.</p> <p>In Intermediate System-to-Intermediate System (IS-IS), there is no backup designated router. Setting the priority to 0 lowers the chance of this system becoming the DIS, but does not prevent it. If a router with a higher priority comes on line, it will take over the role from the current DIS. In the case of equal priorities, the highest MAC address breaks the tie.</p> <p>This command requires the Enterprise Services license.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 4.x (2008), at L3-232.</p>	Syntax Description	<i>number-value</i>	Priority of a router and is a number from 0 to 127. The default value is 64.		level-1	(Optional) Sets the priority for Level 1 independently.		level-2	(Optional) Sets the priority for Level 2 independently.	Command History	Release	Modification		4.0(1)	This command was introduced.	<p>isis priority</p> <p>The isis priority command configures IS-IS router priority for the configuration mode interface.</p> <p>The priority is used to determine which device will be the Designated Intermediate System (DIS). The device with the highest priority will become the DIS.</p> <p>In IS-IS, there is no backup designated router. Setting the priority to 0 lowers the chance of this system becoming the DIS, but does not prevent it. If a device with a higher priority comes on line, it will take over the role from the current DIS.</p> <p>The no isis priority and default isis priority commands restore the default priority (64) on the configuration mode interface.</p> <p>Platform all</p> <p>Command Mode Interface-Ethernet Configuration Interface-Loopback Configuration Interface-Port-channel Configuration Interface-VLAN Configuration</p> <p>Command Syntax</p> <p>isis priority <i>priority_level</i></p> <p>no isis priority</p> <p>default isis priority</p> <p>Parameters</p> <ul style="list-style-type: none"> <i>priority_level</i> priority level. Value ranges from 0 to 127. Default value is 64. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1690.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1450.</p>
Syntax Description	<i>number-value</i>	Priority of a router and is a number from 0 to 127. The default value is 64.															
	level-1	(Optional) Sets the priority for Level 1 independently.															
	level-2	(Optional) Sets the priority for Level 2 independently.															
Command History	Release	Modification															
	4.0(1)	This command was introduced.															

Copyright Registration Information	Cisco	Arista															
<p>Cisco IOS 15.0</p> <p>Effective date of registration: 11/28/2014</p>	<p>isis priority</p> <p>To configure the priority of designated routers, use the isis priority command in interface configuration mode. To reset the default priority, use the no form of this command.</p> <p>isis priority <i>number-value</i> [level-1 level-2]</p> <p>no isis priority [level-1 level-2]</p> <table border="1"> <tr> <td>Syntax Description</td><td><i>number-value</i></td><td>Priority of a router and is a number from 0 to 127. The default value is 64.</td></tr> <tr> <td></td><td>level-1</td><td>(Optional) Sets the priority for Level 1 independently.</td></tr> <tr> <td></td><td>level-2</td><td>(Optional) Sets the priority for Level 2 independently.</td></tr> </table> <p>Defaults</p> <p>Priority of 64 Level 1 and Level 2</p> <p>Command Modes</p> <p>Interface configuration</p> <p>Supported User Roles</p> <p>network-admin vdc-admin</p> <table border="1"> <tr> <td>Command History</td><td>Release</td><td>Modification</td></tr> <tr> <td></td><td>4.0(1)</td><td>This command was introduced.</td></tr> </table> <p>Usage Guidelines</p> <p>Priorities can be configured for Level 1 and Level 2 independently. Specifying the level-1 or level-2 keyword resets priority only for Level 1 or Level 2 routing, respectively.</p> <p>The priority is used to determine which router on a LAN will be the designated router or Designated Intermediate System (DIS). The priorities are advertised in the hello packets. The router with the highest priority will become the DIS.</p> <p>In Intermediate System-to-Intermediate System (IS-IS), there is no backup designated router. Setting the priority to 0 lowers the chance of this system becoming the DIS, but does not prevent it. If a router with a higher priority comes on line, it will take over the role from the current DIS. In the case of equal priorities, the highest MAC address breaks the tie.</p> <p>This command requires the Enterprise Services license.</p> <p>Cisco IOS IP Routing: ISIS Command Reference (2009), at IRS-63.</p>	Syntax Description	<i>number-value</i>	Priority of a router and is a number from 0 to 127. The default value is 64.		level-1	(Optional) Sets the priority for Level 1 independently.		level-2	(Optional) Sets the priority for Level 2 independently.	Command History	Release	Modification		4.0(1)	This command was introduced.	<p>isis priority</p> <p>The isis priority command configures IS-IS router priority for the configuration mode interface.</p> <p>The priority is used to determine which device will be the Designated Intermediate System (DIS). The device with the highest priority will become the DIS.</p> <p>In IS-IS, there is no backup designated router. Setting the priority to 0 lowers the chance of this system becoming the DIS, but does not prevent it. If a device with a higher priority comes on line, it will take over the role from the current DIS.</p> <p>The no isis priority and default isis priority commands restore the default priority (64) on the configuration mode interface.</p> <p>Platform all</p> <p>Command Mode Interface-Ethernet Configuration Interface-Loopback Configuration Interface-Port-channel Configuration Interface-VLAN Configuration</p> <p>Command Syntax</p> <p>isis priority <i>priority_level</i></p> <p>no isis priority</p> <p>default isis priority</p> <p>Parameters</p> <ul style="list-style-type: none"> <i>priority_level</i> priority level. Value ranges from 0 to 127. Default value is 64. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1690.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1450.</p>
Syntax Description	<i>number-value</i>	Priority of a router and is a number from 0 to 127. The default value is 64.															
	level-1	(Optional) Sets the priority for Level 1 independently.															
	level-2	(Optional) Sets the priority for Level 2 independently.															
Command History	Release	Modification															
	4.0(1)	This command was introduced.															

Copyright Registration Information	Cisco	Arista										
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<div>log-adjacency-changes (IS-IS)</div> <p>To enable the router to send a syslog message when an Intermediate System-to-Intermediate System Intradomain Routing Protocol (IS-IS) neighbor goes up or down, use the <code>log-adjacency-changes</code> configuration mode command. To disable this function, use the <code>no</code> form of this command.</p> <div>log-adjacency-changes</div> <div>no log-adjacency-changes</div> <div><div>Syntax Description</div><div>This command has no arguments or keywords.</div></div> <div><div>Defaults</div><div>This command is enabled by default.</div></div> <div><div>Command Modes</div><div>Router configuration VRF configuration</div></div> <div><div>Supported User Roles</div><div>network-admin vdc-admin</div></div> <div><div>Command History</div><table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.0(1)</td><td>This command was introduced.</td></tr></table></div> <div><div>Usage Guidelines</div><div>The <code>log-adjacency-changes</code> command is on by default but only up/down (full/down) events are reported.</div></div> <div><div>Examples</div><div>This example configures the router to send a syslog message when an IS-IS neighbor state changes: switch(config)# router isis switch(config-router)# log-adjacency-changes</div></div> <div><div>Related Commands</div><table><tr><th>Command</th><th>Description</th></tr><tr><td>feature isis</td><td>Enables IS-IS on the router.</td></tr><tr><td>router isis</td><td>Enables IS-IS.</td></tr></table></div>	Release	Modification	4.0(1)	This command was introduced.	Command	Description	feature isis	Enables IS-IS on the router.	router isis	Enables IS-IS.	<div>log-adjacency-changes (IS-IS)</div> <p>The <code>log-adjacency-changes</code> command configures the switch to send syslog messages either when it detects IS-IS link state changes or when it detects that a neighbor has gone up or down. Log message sending is disabled by default.</p> <p>The default option is active when <i>running-config</i> does not contain any form of the command. Entering the command in any form replaces the previous command state in <i>running-config</i>.</p> <div><div>Platform</div><div>all</div></div> <div><div>Command Mode</div><div>Router-IS-IS Configuration</div></div> <div><div>Command Syntax</div><div>log-adjacency-changes</div><div>no log-adjacency-changes</div><div>default log-adjacency-changes</div></div> <div><div>Examples</div><ul style="list-style-type: none">These commands configure the switch to send a syslog message when a neighbor goes up or down. switch(config)#router isis Osiris switch(config-router-isis)#log-adjacency-changes switch(config-router-isis)#These commands configure not to log the peer changes. switch(config)#router isis Osiris switch(config-router-isis)#no log-adjacency-changes switch(config-router-isis)#</div> <div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1692.</div> <div>See also Arista User Manual v. 4.12.3 (7/17/13), at 1452.</div>
	Release	Modification										
4.0(1)	This command was introduced.											
Command	Description											
feature isis	Enables IS-IS on the router.											
router isis	Enables IS-IS.											

Copyright Registration Information	Cisco	Arista										
Cisco NX-OS 5.0 Effective date of registration: 11/13/2014	<div>log-adjacency-changes (IS-IS)</div> <p>To enable the router to send a syslog message when an Intermediate System-to-Intermediate System Intradomain Routing Protocol (IS-IS) neighbor goes up or down, use the log-adjacency-changes configuration mode command. To disable this function, use the no form of this command.</p> <div>log-adjacency-changes</div> <div>no log-adjacency-changes</div> <div><div>Syntax Description</div><div>This command has no arguments or keywords.</div></div> <div><div>Defaults</div><div>This command is enabled by default.</div></div> <div><div>Command Modes</div><div>Router configuration VRF configuration</div></div> <div><div>Supported User Roles</div><div>network-admin vdc-admin</div></div> <div><div>Command History</div><table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.0(1)</td><td>This command was introduced.</td></tr></table></div> <div><div>Usage Guidelines</div><div>The log-adjacency-changes command is on by default but only up/down (full/down) events are reported.</div></div> <div><div>Examples</div><div>This example configures the router to send a syslog message when an IS-IS neighbor state changes: switch(config)# router isis switch(config-router)# log-adjacency-changes</div></div> <div><div>Related Commands</div><table><tr><th>Command</th><th>Description</th></tr><tr><td>feature isis</td><td>Enables IS-IS on the router.</td></tr><tr><td>router isis</td><td>Enables IS-IS.</td></tr></table></div>	Release	Modification	4.0(1)	This command was introduced.	Command	Description	feature isis	Enables IS-IS on the router.	router isis	Enables IS-IS.	<div>log-adjacency-changes (IS-IS)</div> <p>The log-adjacency-changes command configures the switch to send syslog messages either when it detects IS-IS link state changes or when it detects that a neighbor has gone up or down. Log message sending is disabled by default.</p> <p>The default option is active when running-config does not contain any form of the command. Entering the command in any form replaces the previous command state in running-config.</p> <div><div>Platform</div><div>all</div></div> <div><div>Command Mode</div><div>Router-IS-IS Configuration</div></div> <div><div>Command Syntax</div><div>log-adjacency-changes</div><div>no log-adjacency-changes</div><div>default log-adjacency-changes</div></div> <div><div>Examples</div><ul style="list-style-type: none">These commands configure the switch to send a syslog message when a neighbor goes up or down. switch(config)#router isis Osiris switch(config-router-isis)#log-adjacency-changes switch(config-router-isis)#These commands configure not to log the peer changes. switch(config)#router isis Osiris switch(config-router-isis)#no log-adjacency-changes switch(config-router-isis)#</div> <div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1692.</div> <div>See also Arista User Manual v. 4.12.3 (7/17/13), at 1452.</div>
	Release	Modification										
	4.0(1)	This command was introduced.										
	Command	Description										
	feature isis	Enables IS-IS on the router.										
	router isis	Enables IS-IS.										

Copyright Registration Information	Cisco	Arista																														
Cisco NX-OS 4.0 Effective date of registration: 11/13/2014	<div>log-adjacency-changes (IS-IS)</div> <p>To enable the router to send a syslog message when an Intermediate System-to-Intermediate System Intradomain Routing Protocol (IS-IS) neighbor goes up or down, use the <code>log-adjacency-changes</code> configuration mode command. To disable this function, use the no form of this command.</p> <div>log-adjacency-changes</div> <div>no log-adjacency-changes</div> <table><tr><td>Syntax Description</td><td>This command has no arguments or keywords.</td></tr><tr><td>Defaults</td><td>This command is enabled by default.</td></tr><tr><td>Command Modes</td><td>Router configuration VRF configuration</td></tr><tr><td>Supported User Roles</td><td>network-admin vdc-admin</td></tr><tr><td>Command History</td><td><table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.0(1)</td><td>This command was introduced.</td></tr></table></td></tr><tr><td>Usage Guidelines</td><td>The <code>log-adjacency-changes</code> command is on by default but only up/down (full/down) events are reported.</td></tr><tr><td>Examples</td><td>This example configures the router to send a syslog message when an IS-IS neighbor state changes: <pre>switch(config)# router isis switch(config-router)# log-adjacency-changes</pre></td></tr><tr><td>Related Commands</td><td><table><tr><th>Command</th><th>Description</th></tr><tr><td>feature isis</td><td>Enables IS-IS on the router.</td></tr><tr><td>router isis</td><td>Enables IS-IS.</td></tr></table></td></tr></table>	Syntax Description	This command has no arguments or keywords.	Defaults	This command is enabled by default.	Command Modes	Router configuration VRF configuration	Supported User Roles	network-admin vdc-admin	Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.0(1)</td><td>This command was introduced.</td></tr></table>	Release	Modification	4.0(1)	This command was introduced.	Usage Guidelines	The <code>log-adjacency-changes</code> command is on by default but only up/down (full/down) events are reported.	Examples	This example configures the router to send a syslog message when an IS-IS neighbor state changes: <pre>switch(config)# router isis switch(config-router)# log-adjacency-changes</pre>	Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>feature isis</td><td>Enables IS-IS on the router.</td></tr><tr><td>router isis</td><td>Enables IS-IS.</td></tr></table>	Command	Description	feature isis	Enables IS-IS on the router.	router isis	Enables IS-IS.	<div>log-adjacency-changes (IS-IS)</div> <p>The <code>log-adjacency-changes</code> command configures the switch to send syslog messages either when it detects IS-IS link state changes or when it detects that a neighbor has gone up or down. Log message sending is disabled by default.</p> <p>The default option is active when <i>running-config</i> does not contain any form of the command. Entering the command in any form replaces the previous command state in <i>running-config</i>.</p> <table><tr><td>Platform</td><td>all</td></tr><tr><td>Command Mode</td><td>Router-IS-IS Configuration</td></tr></table> <p>Command Syntax</p> <div>log-adjacency-changes</div> <div>no log-adjacency-changes</div> <div>default log-adjacency-changes</div> <p>Examples</p> <ul style="list-style-type: none">These commands configure the switch to send a syslog message when a neighbor goes up or down. <pre>switch(config)#router isis Osiris switch(config-router-isis)#log-adjacency-changes switch(config-router-isis)#</pre>These commands configure not to log the peer changes. <pre>switch(config)#router isis Osiris switch(config-router-isis)#no log-adjacency-changes switch(config-router-isis)#</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1692.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1452.</p>	Platform	all	Command Mode	Router-IS-IS Configuration
	Syntax Description	This command has no arguments or keywords.																														
	Defaults	This command is enabled by default.																														
	Command Modes	Router configuration VRF configuration																														
	Supported User Roles	network-admin vdc-admin																														
	Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.0(1)</td><td>This command was introduced.</td></tr></table>	Release	Modification	4.0(1)	This command was introduced.																										
	Release	Modification																														
	4.0(1)	This command was introduced.																														
	Usage Guidelines	The <code>log-adjacency-changes</code> command is on by default but only up/down (full/down) events are reported.																														
	Examples	This example configures the router to send a syslog message when an IS-IS neighbor state changes: <pre>switch(config)# router isis switch(config-router)# log-adjacency-changes</pre>																														
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>feature isis</td><td>Enables IS-IS on the router.</td></tr><tr><td>router isis</td><td>Enables IS-IS.</td></tr></table>	Command	Description	feature isis	Enables IS-IS on the router.	router isis	Enables IS-IS.																									
Command	Description																															
feature isis	Enables IS-IS on the router.																															
router isis	Enables IS-IS.																															
Platform	all																															
Command Mode	Router-IS-IS Configuration																															

Copyright Registration Information	Cisco	Arista																				
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<div>max-metric router-lsa (OSPF)</div> <div><p>To configure the Open Shortest Path First (OSPF) protocol to advertise a maximum metric so that other routers do not prefer the router as an intermediate hop in their shortest path first (SPF) calculations, use the max-metric router-lsa command. To disable the advertisement of a maximum metric, use the no form of this command.</p><pre>max-metric router-lsa [external-lsa [max-metric-value]] [include-stub] [on-startup [seconds] wait-for bgp tag] [summary-lsa [max-metric-value]]</pre><pre>no max-metric router-lsa [external-lsa [max-metric-value]] [include-stub] [on-startup [seconds] wait-for bgp tag] [summary-lsa [max-metric-value]]</pre><table><tr><td>external-lsa</td><td>Specifies the external LSA's.</td></tr><tr><td>max-metric-value</td><td>(Optional) Specifies the max-metric values for external LSA's. The range is 1-65535.</td></tr><tr><td>include-stub</td><td>Advertises the max-metric for stub links.</td></tr><tr><td>on-startup</td><td>(Optional) Configures the router to advertise a maximum metric at startup.</td></tr><tr><td>seconds</td><td>(Optional) Maximum metric (in seconds) that is advertised for the specified time interval. The configurable range is from 5 to 86400 seconds. The default is 600 seconds.</td></tr><tr><td>wait-for bgp tag</td><td>(Optional) Advertises a maximum metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired. The default timer is 600 seconds.</td></tr><tr><td>summary-lsa</td><td>Specifies the summary LSA's.</td></tr><tr><td>max-metric-value</td><td>(Optional) Specifies the max-metric value for summary LSAs. The range is from 1-65535.</td></tr></table><div><div>Defaults</div><div>Originates router link-state advertisements (LSAs) with normal link metrics.</div></div><div><div>Command Modes</div><div>Router configuration Router VRF configuration</div></div><div><div>Supported User Roles</div><div>network-admin vdc-admin</div></div><div><div>Command History</div><table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.0(1)</td><td>This command was introduced.</td></tr></table></div></div> <div>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference (2013), at 194.</div>	external-lsa	Specifies the external LSA's.	max-metric-value	(Optional) Specifies the max-metric values for external LSA's. The range is 1-65535.	include-stub	Advertises the max-metric for stub links.	on-startup	(Optional) Configures the router to advertise a maximum metric at startup.	seconds	(Optional) Maximum metric (in seconds) that is advertised for the specified time interval. The configurable range is from 5 to 86400 seconds. The default is 600 seconds.	wait-for bgp tag	(Optional) Advertises a maximum metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired. The default timer is 600 seconds.	summary-lsa	Specifies the summary LSA's.	max-metric-value	(Optional) Specifies the max-metric value for summary LSAs. The range is from 1-65535.	Release	Modification	4.0(1)	This command was introduced.	<div>max-metric router-lsa (OSPFv2)</div> <div><p>The max-metric router-lsa command allows the OSPF protocol to advertise a maximum metric so that other routers do not prefer the router as an intermediate hop in their SPF calculations.</p><p>The no max-metric router-lsa and default max-metric router-lsa commands disable the advertisement of a maximum metric.</p><div><div>Platform</div><div>all</div></div><div><div>Command Mode</div><div>Router-OSPF Configuration</div></div><div><div>Command Syntax</div><pre>max-metric router-lsa [EXTERNAL] [STUB] [STARTUP] [SUMMARY]</pre><pre>no max-metric router-lsa [EXTERNAL] [STUB] [STARTUP] [SUMMARY]</pre><pre>default max-metric router-lsa [EXTERNAL] [STUB] [STARTUP] [SUMMARY]</pre><p>All parameters can be placed in any order.</p><div><div>Parameters</div><ul style="list-style-type: none">EXTERNAL advertised metric value. Values include:<ul style="list-style-type: none"><no parameter> Metric is set to the default value of 1.external-lsa Configures the router to override the External LSA / NSSA-External metric with the maximum metric value.external-lsa <1 to 16777215> The configurable range is from 1 to 0xFFFFF. The default value is 0xFF0000. This range can be used with external LSA, summary LSA extensions to indicate the respective metric you want with the LSA.STUB advertised metric type. Values include:<ul style="list-style-type: none"><no parameter> Metric type is set to the default value of 2.include-stub Advertises stub links in router-LSA with the max-metric value (0xFFFF).STARTUP limit scope of LSAs. Values include:<ul style="list-style-type: none"><no parameter> LSA can be translatedon-startup Configures the router to advertise a maximum metric at startup (only valid in no and default command formats).on-startup wait-for-bgp Configures the router to advertise a maximum metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired. The default timer is 600 seconds.on-startup <5 to 86400> Sets the maximum metric temporarily after a reboot to originate router LSAs with the max-metric value.wait-for-bgp or an on-start time value is not included in no and default commands.SUMMARY advertised metric value. Values include:<ul style="list-style-type: none"><no parameter> Metric is set to the default value of 1.summary-lsa Configures the router to override the summary LSA metric with the maximum metric value for both type 3 and type 4 Summary LSAs.summary-lsa <1 to 16777215> Metric is set to the specified value.</div></div></div> <div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1439.</div>
	external-lsa	Specifies the external LSA's.																				
max-metric-value	(Optional) Specifies the max-metric values for external LSA's. The range is 1-65535.																					
include-stub	Advertises the max-metric for stub links.																					
on-startup	(Optional) Configures the router to advertise a maximum metric at startup.																					
seconds	(Optional) Maximum metric (in seconds) that is advertised for the specified time interval. The configurable range is from 5 to 86400 seconds. The default is 600 seconds.																					
wait-for bgp tag	(Optional) Advertises a maximum metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired. The default timer is 600 seconds.																					
summary-lsa	Specifies the summary LSA's.																					
max-metric-value	(Optional) Specifies the max-metric value for summary LSAs. The range is from 1-65535.																					
Release	Modification																					
4.0(1)	This command was introduced.																					

<div>Copyright Registration Information</div>	<div>Cisco</div> <div><div>max-metric router-lsa (OSPF)</div><div><div>To configure the Open Shortest Path First (OSPF) protocol to advertise a maximum metric so that other routers do not prefer the router as an intermediate hop in their shortest path first (SPF) calculations, use the max-metric router-lsa command. To disable the advertisement of a maximum metric, use the no form of this command.</div><div><div><div>max-metric router-lsa [external-lsa [max-metric-value]] [include-stub] [on-startup [seconds] wait-for bgp tag]] summary-lsa [max-metric-value]]</div><div><div>no max-metric router-lsa [external-lsa [max-metric-value]] [include-stub] [on-startup [seconds] wait-for bgp tag]] summary-lsa [max-metric-value]]</div></div><table><tr><td>external-lsa</td><td>Specifies the external LSA's.</td></tr><tr><td>max-metric-value</td><td>(Optional) Specifies the max-metric values for external LSA's. The range is 1-65535.</td></tr><tr><td>include-stub</td><td>Advertises the max-metric for stub links.</td></tr><tr><td>on-startup</td><td>(Optional) Configures the router to advertise a maximum metric at startup.</td></tr><tr><td>seconds</td><td>(Optional) Maximum metric (in seconds) that is advertised for the specified time interval. The configurable range is from 5 to 86400 seconds. The default is 600 seconds.</td></tr><tr><td>wait-for bgp tag</td><td>(Optional) Advertises a maximum metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired. The default timer is 600 seconds.</td></tr><tr><td>summary-lsa</td><td>Specifies the summary LSA's.</td></tr><tr><td>max-metric-value</td><td>(Optional) Specifies the max-metric value for summary LSAs. The range is from 1-65535.</td></tr></table><div><div>Defaults</div><div>Originates router link-state advertisements (LSAs) with normal link metrics.</div></div><div><div>Command Modes</div><div>Router configuration Router VRF configuration</div></div><div><div>Supported User Roles</div><div>network-admin vdc-admin</div></div><div><div>Command History</div><table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.0(1)</td><td>This command was introduced.</td></tr></table></div></div><div><div>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 5.x (2010), at L3-457</div></div></div></div></div>	external-lsa	Specifies the external LSA's.	max-metric-value	(Optional) Specifies the max-metric values for external LSA's. The range is 1-65535.	include-stub	Advertises the max-metric for stub links.	on-startup	(Optional) Configures the router to advertise a maximum metric at startup.	seconds	(Optional) Maximum metric (in seconds) that is advertised for the specified time interval. The configurable range is from 5 to 86400 seconds. The default is 600 seconds.	wait-for bgp tag	(Optional) Advertises a maximum metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired. The default timer is 600 seconds.	summary-lsa	Specifies the summary LSA's.	max-metric-value	(Optional) Specifies the max-metric value for summary LSAs. The range is from 1-65535.	Release	Modification	4.0(1)	This command was introduced.	<div>Arista</div> <div><div>max-metric router-lsa (OSPFv2)</div><div><div>The max-metric router-lsa command allows the OSPF protocol to advertise a maximum metric so that other routers do not prefer the router as an intermediate hop in their SPF calculations.</div><div><div>The no max-metric router-lsa and default max-metric router-lsa commands disable the advertisement of a maximum metric.</div><div><div>Platform all</div><div>Command Mode Router-OSPF Configuration</div></div><div><div>Command Syntax</div><div><div>max-metric router-lsa [EXTERNAL] [STUB] [STARTUP] [SUMMARY]</div><div><div>no max-metric router-lsa [EXTERNAL] [STUB] [STARTUP] [SUMMARY]</div><div><div>default max-metric router-lsa [EXTERNAL] [STUB] [STARTUP] [SUMMARY]</div></div></div><div><div>All parameters can be placed in any order.</div></div><div><div>Parameters</div><div><div><div><div>EXTERNAL</div><div>advertised metric value. Values include:</div><div><div><div><no parameter></div><div>Metric is set to the default value of 1.</div></div><div><div>external-lsa</div><div>Configures the router to override the External LSA / NSSA-External metric with the maximum metric value.</div></div><div><div>external-lsa <1 to 16777215></div><div>The configurable range is from 1 to 0xFFFFF. The default value is 0xFF0000. This range can be used with external LSA, summary LSA extensions to indicate the respective metric you want with the LSA.</div></div></div></div><div><div><div>STUB</div><div>advertised metric type. Values include:</div><div><div><div><no parameter></div><div>Metric type is set to the default value of 2.</div></div><div><div>include-stub</div><div>Advertises stub links in router-LSA with the max-metric value (0xFFFF).</div></div></div></div><div><div><div>STARTUP</div><div>limit scope of LSAs. Values include:</div><div><div><div><no parameter></div><div>LSA can be translated</div></div><div><div>on-startup</div><div>Configures the router to advertise a maximum metric at startup (only valid in no and default command formats).</div></div><div><div>on-startup wait-for-bgp</div><div>Configures the router to advertise a maximum metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired. The default timer is 600 seconds.</div></div><div><div>on-startup <5 to 86400></div><div>Sets the maximum metric temporarily after a reboot to originate router LSAs with the max-metric value.</div></div><div><div>wait-for-bgp</div><div>or an on-start time value is not included in no and default commands.</div></div></div></div><div><div><div>SUMMARY</div><div>advertised metric value. Values include:</div><div><div><div><no parameter></div><div>Metric is set to the default value of 1.</div></div><div><div>summary-lsa</div><div>Configures the router to override the summary LSA metric with the maximum metric value for both type 3 and type 4 Summary LSAs.</div></div><div><div>summary-lsa <1 to 16777215></div><div>Metric is set to the specified value.</div></div></div></div></div></div></div></div></div></div></div></div></div></div></div>	<div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1439.</div>
external-lsa	Specifies the external LSA's.																						
max-metric-value	(Optional) Specifies the max-metric values for external LSA's. The range is 1-65535.																						
include-stub	Advertises the max-metric for stub links.																						
on-startup	(Optional) Configures the router to advertise a maximum metric at startup.																						
seconds	(Optional) Maximum metric (in seconds) that is advertised for the specified time interval. The configurable range is from 5 to 86400 seconds. The default is 600 seconds.																						
wait-for bgp tag	(Optional) Advertises a maximum metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired. The default timer is 600 seconds.																						
summary-lsa	Specifies the summary LSA's.																						
max-metric-value	(Optional) Specifies the max-metric value for summary LSAs. The range is from 1-65535.																						
Release	Modification																						
4.0(1)	This command was introduced.																						

Copyright Registration Information	Cisco	Arista																				
Cisco NX-OS 4.0 Effective date of registration: 11/13/2014	<div>max-metric router-lsa (OSPF)</div> <div><p>To configure the Open Shortest Path First (OSPF) protocol to advertise a maximum metric so that other routers do not prefer the router as an intermediate hop in their shortest path first (SPF) calculations, use the max-metric router-lsa command. To disable the advertisement of a maximum metric, use the no form of this command.</p><pre>max-metric router-lsa [external-lsa [max-metric-value]] [include-stub] [on-startup [seconds] wait-for bgp tag]] summary-lsa [max-metric-value]] no max-metric router-lsa [external-lsa [max-metric-value]] [include-stub] [on-startup [seconds] wait-for bgp tag]] summary-lsa [max-metric-value]]</pre><table><tr><td>external-lsa</td><td>Specifies the external LSA's.</td></tr><tr><td>max-metric-value</td><td>(Optional) Specifies the max-metric values for external LSA's. The range is 1-65535.</td></tr><tr><td>include-stub</td><td>Advertises the max-metric for stub links.</td></tr><tr><td>on-startup</td><td>(Optional) Configures the router to advertise a maximum metric at startup.</td></tr><tr><td>seconds</td><td>(Optional) Maximum metric (in seconds) that is advertised for the specified time interval. The configurable range is from 5 to 86400 seconds. The default is 600 seconds.</td></tr><tr><td>wait-for bgp tag</td><td>(Optional) Advertises a maximum metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired. The default timer is 600 seconds.</td></tr><tr><td>summary-lsa</td><td>Specifies the summary LSA's.</td></tr><tr><td>max-metric-value</td><td>(Optional) Specifies the max-metric value for summary LSAs. The range is from 1-65535.</td></tr></table><div><div>Defaults</div><div>Originates router link-state advertisements (LSAs) with normal link metrics.</div></div><div><div>Command Modes</div><div>Router configuration Router VRF configuration</div></div><div><div>Supported User Roles</div><div>network-admin vdc-admin</div></div><div><div>Command History</div><table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.0(1)</td><td>This command was introduced.</td></tr></table></div></div>	external-lsa	Specifies the external LSA's.	max-metric-value	(Optional) Specifies the max-metric values for external LSA's. The range is 1-65535.	include-stub	Advertises the max-metric for stub links.	on-startup	(Optional) Configures the router to advertise a maximum metric at startup.	seconds	(Optional) Maximum metric (in seconds) that is advertised for the specified time interval. The configurable range is from 5 to 86400 seconds. The default is 600 seconds.	wait-for bgp tag	(Optional) Advertises a maximum metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired. The default timer is 600 seconds.	summary-lsa	Specifies the summary LSA's.	max-metric-value	(Optional) Specifies the max-metric value for summary LSAs. The range is from 1-65535.	Release	Modification	4.0(1)	This command was introduced.	<div>max-metric router-lsa (OSPFv2)</div> <div><p>The max-metric router-lsa command allows the OSPF protocol to advertise a maximum metric so that other routers do not prefer the router as an intermediate hop in their SPF calculations.</p><p>The no max-metric router-lsa and default max-metric router-lsa commands disable the advertisement of a maximum metric.</p><div><div>Platform</div><div>all</div></div><div><div>Command Mode</div><div>Router-OSPF Configuration</div></div><div><div>Command Syntax</div><pre>max-metric router-lsa [EXTERNAL] [STUB] [STARTUP] [SUMMARY] no max-metric router-lsa [EXTERNAL] [STUB] [STARTUP] [SUMMARY] default max-metric router-lsa [EXTERNAL] [STUB] [STARTUP] [SUMMARY]</pre><p>All parameters can be placed in any order.</p><div><div>Parameters</div><div><ul style="list-style-type: none">EXTERNAL advertised metric value. Values include:<ul style="list-style-type: none"><no parameter> Metric is set to the default value of 1.external-lsa Configures the router to override the External LSA / NSSA-External metric with the maximum metric value.external-lsa <1 to 16777215> The configurable range is from 1 to 0xFFFFFE. The default value is 0xFF0000. This range can be used with external LSA, summary LSA extensions to indicate the respective metric you want with the LSA.STUB advertised metric type. Values include:<ul style="list-style-type: none"><no parameter> Metric type is set to the default value of 2.include-stub Advertises stub links in router-LSA with the max-metric value (0xFFFF).STARTUP limit scope of LSAs. Values include:<ul style="list-style-type: none"><no parameter> LSA can be translatedon-startup Configures the router to advertise a maximum metric at startup (only valid in no and default command formats).on-startup wait-for-bgp Configures the router to advertise a maximum metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired. The default timer is 600 seconds.on-startup <5 to 86400> Sets the maximum metric temporarily after a reboot to originate router LSAs with the max-metric value.wait-for-bgp or an on-start time value is not included in no and default commands.SUMMARY advertised metric value. Values include:<ul style="list-style-type: none"><no parameter> Metric is set to the default value of 1.summary-lsa Configures the router to override the summary LSA metric with the maximum metric value for both type 3 and type 4 Summary LSAs.summary-lsa <1 to 16777215> Metric is set to the specified value.</div></div></div></div>
	external-lsa	Specifies the external LSA's.																				
max-metric-value	(Optional) Specifies the max-metric values for external LSA's. The range is 1-65535.																					
include-stub	Advertises the max-metric for stub links.																					
on-startup	(Optional) Configures the router to advertise a maximum metric at startup.																					
seconds	(Optional) Maximum metric (in seconds) that is advertised for the specified time interval. The configurable range is from 5 to 86400 seconds. The default is 600 seconds.																					
wait-for bgp tag	(Optional) Advertises a maximum metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired. The default timer is 600 seconds.																					
summary-lsa	Specifies the summary LSA's.																					
max-metric-value	(Optional) Specifies the max-metric value for summary LSAs. The range is from 1-65535.																					
Release	Modification																					
4.0(1)	This command was introduced.																					

Copyright Registration Information	Cisco	Arista																					
Cisco IOS 15.0 Effective date of registration: 11/28/2014	<div>max-metric router-lsa (OSPF)</div> <div><p>To configure the Open Shortest Path First (OSPF) protocol to advertise a maximum metric so that other routers do not prefer the router as an intermediate hop in their shortest path first (SPF) calculations, use the <code>max-metric router-lsa</code> command. To disable the advertisement of a maximum metric, use the <code>no</code> form of this command.</p><pre>max-metric router-lsa [external-lsa [max-metric-value]] [include-stub] [on-startup [seconds] wait-for bgp tag]] [summary-lsa [max-metric-value]]</pre><pre>no max-metric router-lsa [external-lsa [max-metric-value]] [include-stub] [on-startup [seconds] wait-for bgp tag]] [summary-lsa [max-metric-value]]</pre><table><tr><td><code>external-lsa</code></td><td>Specifies the external LSA's.</td></tr><tr><td><code>max-metric-value</code></td><td>(Optional) Specifies the max-metric values for external LSA's. The range is 1-65535.</td></tr><tr><td><code>include-stub</code></td><td>Advertises the max-metric for stub links.</td></tr><tr><td><code>on-startup</code></td><td>(Optional) Configures the router to advertise a maximum metric at startup.</td></tr><tr><td><code>seconds</code></td><td>(Optional) Maximum metric (in seconds) that is advertised for the specified time interval. The configurable range is from 5 to 86400 seconds. The default is 600 seconds.</td></tr><tr><td><code>wait-for bgp tag</code></td><td>(Optional) Advertises a maximum metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired. The default timer is 600 seconds.</td></tr><tr><td><code>summary-lsa</code></td><td>Specifies the summary LSA's.</td></tr><tr><td><code>max-metric-value</code></td><td>(Optional) Specifies the max-metric value for summary LSAs. The range is from 1-65535.</td></tr></table><div><div>Defaults</div><div>Originates router link-state advertisements (LSAs) with normal link metrics.</div></div><div><div>Command Modes</div><div>Router configuration Router VRF configuration</div></div><div><div>Supported User Roles</div><div>network-admin vdc-admin</div></div><div><div>Command History</div><table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.0(1)</td><td>This command was introduced.</td></tr></table></div></div>	<code>external-lsa</code>	Specifies the external LSA's.	<code>max-metric-value</code>	(Optional) Specifies the max-metric values for external LSA's. The range is 1-65535.	<code>include-stub</code>	Advertises the max-metric for stub links.	<code>on-startup</code>	(Optional) Configures the router to advertise a maximum metric at startup.	<code>seconds</code>	(Optional) Maximum metric (in seconds) that is advertised for the specified time interval. The configurable range is from 5 to 86400 seconds. The default is 600 seconds.	<code>wait-for bgp tag</code>	(Optional) Advertises a maximum metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired. The default timer is 600 seconds.	<code>summary-lsa</code>	Specifies the summary LSA's.	<code>max-metric-value</code>	(Optional) Specifies the max-metric value for summary LSAs. The range is from 1-65535.	Release	Modification	4.0(1)	This command was introduced.	<div>max-metric router-lsa (OSPFv2)</div> <div><p>The <code>max-metric router-lsa</code> command allows the OSPF protocol to advertise a maximum metric so that other routers do not prefer the router as an intermediate hop in their SPF calculations.</p><p>The <code>no max-metric router-lsa</code> and <code>default max-metric router-lsa</code> commands disable the advertisement of a maximum metric.</p><div><div>Platform</div><div>all</div></div><div><div>Command Mode</div><div>Router-OSPF Configuration</div></div><div><div>Command Syntax</div><pre>max-metric router-lsa [EXTERNAL] [STUB] [STARTUP] [SUMMARY] no max-metric router-lsa [EXTERNAL] [STUB] [STARTUP] [SUMMARY] default max-metric router-lsa [EXTERNAL] [STUB] [STARTUP] [SUMMARY]</pre><p>All parameters can be placed in any order.</p><div><div>Parameters</div><ul style="list-style-type: none"><div><code>EXTERNAL</code></div><div>advertised metric value. Values include:</div><ul style="list-style-type: none"><code><no parameter></code> Metric is set to the default value of 1.<code>external-lsa</code> Configures the router to override the External LSA / NSSA-External metric with the maximum metric value.<code>external-lsa <1 to 16777215></code> The configurable range is from 1 to 0xFFFFFE. The default value is 0xFF0000. This range can be used with external LSA, summary LSA extensions to indicate the respective metric you want with the LSA.<div><code>STUB</code></div><div>advertised metric type. Values include:</div><ul style="list-style-type: none"><code><no parameter></code> Metric type is set to the default value of 2.<code>include-stub</code> Advertises stub links in router-LSA with the max-metric value (0xFFFF).<div><code>STARTUP</code></div><div>limit scope of LSAs. Values include:</div><ul style="list-style-type: none"><code><no parameter></code> LSA can be translated<code>on-startup</code> Configures the router to advertise a maximum metric at startup (only valid in <code>no</code> and <code>default</code> command formats).<code>on-startup wait-for-bgp</code> Configures the router to advertise a maximum metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired. The default timer is 600 seconds.<code>on-startup <5 to 86400></code> Sets the maximum metric temporarily after a reboot to originate router LSAs with the max-metric value.<code>wait-for-bgp</code> or an on-start time value is not included in <code>no</code> and <code>default</code> commands.<div><code>SUMMARY</code></div><div>advertised metric value. Values include:</div><ul style="list-style-type: none"><code><no parameter></code> Metric is set to the default value of 1.<code>summary-lsa</code> Configures the router to override the summary LSA metric with the maximum metric value for both type 3 and type 4 Summary LSAs.<code>summary-lsa <1 to 16777215></code> Metric is set to the specified value.</div></div></div>	Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1439.
	<code>external-lsa</code>	Specifies the external LSA's.																					
<code>max-metric-value</code>	(Optional) Specifies the max-metric values for external LSA's. The range is 1-65535.																						
<code>include-stub</code>	Advertises the max-metric for stub links.																						
<code>on-startup</code>	(Optional) Configures the router to advertise a maximum metric at startup.																						
<code>seconds</code>	(Optional) Maximum metric (in seconds) that is advertised for the specified time interval. The configurable range is from 5 to 86400 seconds. The default is 600 seconds.																						
<code>wait-for bgp tag</code>	(Optional) Advertises a maximum metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired. The default timer is 600 seconds.																						
<code>summary-lsa</code>	Specifies the summary LSA's.																						
<code>max-metric-value</code>	(Optional) Specifies the max-metric value for summary LSAs. The range is from 1-65535.																						
Release	Modification																						
4.0(1)	This command was introduced.																						

Copyright Registration Information	Cisco	Arista																																																												
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<p>BGP table version is 10, local router ID is 3.3.3.3 Status: s-suppressed, x-deleted, S-stale, d-dampened, h-history, *-valid, >-best Path type: i-internal, e-external, c-confed, l-local, a-aggregate, r-redist Origin codes: i - IGP, e - BGP, ? - incomplete - multipath</p> <table><tr><th>Network</th><th>Next Hop</th><th>Metric</th><th>LocPrf</th><th>Weight</th><th>Path</th></tr><tr><td>* i200.0.1.100/32</td><td>201.0.25.1</td><td></td><td>100</td><td>100</td><td>6553601 i</td></tr><tr><td>*>e</td><td>201.0.13.1</td><td></td><td></td><td>0</td><td>6553601 i</td></tr><tr><td>* i200.0.2.100/32</td><td>201.0.25.1</td><td></td><td>100</td><td>100</td><td>6553601 i</td></tr><tr><td>*>e</td><td>201.0.13.1</td><td></td><td></td><td>0</td><td>6553601 i</td></tr><tr><td>*>i200.0.3.100/32</td><td>0.0.0.0</td><td></td><td>100</td><td>32768</td><td>i</td></tr></table> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference (2013), at 401.</p>	Network	Next Hop	Metric	LocPrf	Weight	Path	* i200.0.1.100/32	201.0.25.1		100	100	6553601 i	*>e	201.0.13.1			0	6553601 i	* i200.0.2.100/32	201.0.25.1		100	100	6553601 i	*>e	201.0.13.1			0	6553601 i	*>i200.0.3.100/32	0.0.0.0		100	32768	i	<p>switch>show ip bgp neighbors 10.14.4.4 advertised-routes regexp _64502_ BGP routing table information for VRF default Router identifier 172.24.78.191, local AS number 64498 Route status codes: s - suppressed, * - valid, > - active, E - ECMP head, e - ECMP S - Stale Origin codes: i - IGP, e - BGP, ? - incomplete AS Path Attributes: Or-ID - Originator ID, C-LST - Cluster List, LL Nexthop - Link Local Nexthop</p> <table><tr><th>Network</th><th>Next Hop</th><th>Metric</th><th>LocPrf</th><th>Weight</th><th>Path</th></tr><tr><td>* > 10.99.31.0/24</td><td>10.88.202.1</td><td>333</td><td>100</td><td>-</td><td>(64502 64503) 99 1</td></tr><tr><td>* > 10.99.41.0/24</td><td>10.88.202.1</td><td>333</td><td>100</td><td>-</td><td>(64502 64503) 99 1</td></tr><tr><td>* > 10.99.99.0/24</td><td>10.88.202.1</td><td>333</td><td>100</td><td>-</td><td>(64502 64504) 99 1</td></tr></table> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1637.</p>	Network	Next Hop	Metric	LocPrf	Weight	Path	* > 10.99.31.0/24	10.88.202.1	333	100	-	(64502 64503) 99 1	* > 10.99.41.0/24	10.88.202.1	333	100	-	(64502 64503) 99 1	* > 10.99.99.0/24	10.88.202.1	333	100	-	(64502 64504) 99 1
Network	Next Hop	Metric	LocPrf	Weight	Path																																																									
* i200.0.1.100/32	201.0.25.1		100	100	6553601 i																																																									
*>e	201.0.13.1			0	6553601 i																																																									
* i200.0.2.100/32	201.0.25.1		100	100	6553601 i																																																									
*>e	201.0.13.1			0	6553601 i																																																									
*>i200.0.3.100/32	0.0.0.0		100	32768	i																																																									
Network	Next Hop	Metric	LocPrf	Weight	Path																																																									
* > 10.99.31.0/24	10.88.202.1	333	100	-	(64502 64503) 99 1																																																									
* > 10.99.41.0/24	10.88.202.1	333	100	-	(64502 64503) 99 1																																																									
* > 10.99.99.0/24	10.88.202.1	333	100	-	(64502 64504) 99 1																																																									
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<p>show ip bgp neighbors</p> <p>To display Border Gateway Protocol (BGP) neighbors, use the show ip bgp neighbors command.</p> <p>show ip bgp neighbors [addr] [advertised-routes] [flap-statistics] [paths] [received-routes] [routes] [advertised] [dampened] [received]] [prefix] [vrf] [all] [vrf-name]]</p> <table><tr><th>Syntax</th><th>Description</th></tr><tr><td>addr</td><td>IPv4 address. The format is x.x.x.x</td></tr><tr><td>advertised-routes</td><td>(Optional) Displays all the routes advertised to this neighbor.</td></tr><tr><td>flap-statistics</td><td>(Optional) Displays flap statistics for the routes received from this neighbor.</td></tr><tr><td>paths</td><td>(Optional) Displays AS paths learned from this neighbor.</td></tr><tr><td>received-routes</td><td>(Optional) Displays all the routes received from this neighbor.</td></tr><tr><td>routes</td><td>(Optional) Displays the routes received or advertised to or from this neighbor.</td></tr><tr><td>advertised</td><td>(Optional) Displays all the routes advertised for this neighbor.</td></tr><tr><td>dampened</td><td>(Optional) Displays all dampened routes received from this neighbor.</td></tr><tr><td>received</td><td>(Optional) Displays all the routes received from this neighbor.</td></tr><tr><td>prefix</td><td>(Optional) IPv6 prefix. The format is x.x.x.x/length</td></tr><tr><td>vrf vrf-name</td><td>(Optional) Specifies the virtual router context (VRF) name. The name can be any case-sensitive, alphanumeric string up to 63 characters.</td></tr><tr><td>all</td><td>(Optional) Specifies all VRF.</td></tr></table> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference (2013), at 466.</p>	Syntax	Description	addr	IPv4 address. The format is x.x.x.x	advertised-routes	(Optional) Displays all the routes advertised to this neighbor.	flap-statistics	(Optional) Displays flap statistics for the routes received from this neighbor.	paths	(Optional) Displays AS paths learned from this neighbor.	received-routes	(Optional) Displays all the routes received from this neighbor.	routes	(Optional) Displays the routes received or advertised to or from this neighbor.	advertised	(Optional) Displays all the routes advertised for this neighbor.	dampened	(Optional) Displays all dampened routes received from this neighbor.	received	(Optional) Displays all the routes received from this neighbor.	prefix	(Optional) IPv6 prefix. The format is x.x.x.x/length	vrf vrf-name	(Optional) Specifies the virtual router context (VRF) name. The name can be any case-sensitive, alphanumeric string up to 63 characters.	all	(Optional) Specifies all VRF.	<p>show ip bgp neighbors</p> <p>The show ip bgp neighbors command displays Border Gateway Protocol (BGP) and TCP session data for a specified IPv4 BGP neighbor, or for all IPv4 BGP neighbors if an address is not included.</p> <p>Platform all Command Mode EXEC</p> <p>Command Syntax</p> <p>show ip bgp neighbors [NEIGHBOR_ADDR] [VRF_INSTANCE]</p> <p>Parameters</p> <ul style="list-style-type: none">NEIGHBOR_ADDR location of neighbors. Options include:<ul style="list-style-type: none"><no parameter> command displays information for all IPv4 BGP neighbors.ipv4 addr command displays information for specified neighbor.VRF_INSTANCE specifies VRF instances.<ul style="list-style-type: none"><no parameter> displays routing table for context-active VRF.vrf vrf_name displays routing table for the specified VRF.vrf all displays routing table for all VRFs.vrf default displays routing table for default VRF. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1632.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1402; Arista User Manual, v. 4.11.1 (1/11/13), at 1148; Arista User Manual v. 4.10.3 (10/22/12), at 959.</p>																																		
Syntax	Description																																																													
addr	IPv4 address. The format is x.x.x.x																																																													
advertised-routes	(Optional) Displays all the routes advertised to this neighbor.																																																													
flap-statistics	(Optional) Displays flap statistics for the routes received from this neighbor.																																																													
paths	(Optional) Displays AS paths learned from this neighbor.																																																													
received-routes	(Optional) Displays all the routes received from this neighbor.																																																													
routes	(Optional) Displays the routes received or advertised to or from this neighbor.																																																													
advertised	(Optional) Displays all the routes advertised for this neighbor.																																																													
dampened	(Optional) Displays all dampened routes received from this neighbor.																																																													
received	(Optional) Displays all the routes received from this neighbor.																																																													
prefix	(Optional) IPv6 prefix. The format is x.x.x.x/length																																																													
vrf vrf-name	(Optional) Specifies the virtual router context (VRF) name. The name can be any case-sensitive, alphanumeric string up to 63 characters.																																																													
all	(Optional) Specifies all VRF.																																																													

Copyright Registration Information	Cisco	Arista																										
	<div>show ip bgp neighbors</div> <div>To display Border Gateway Protocol (BGP) neighbors, use the show ip bgp neighbors command.</div> <div>show ip bgp neighbors [addr] [advertised-routes] [flap-statistics] [paths] [received-routes] [routes] [advertised] [dampened] [received] [prefix] [vrf] [all] [vrf-name]</div> <table><tr><th>Syntax</th><th>Description</th></tr><tr><td>addr</td><td>IPv4 address. The format is x.x.x.x.</td></tr><tr><td>advertised-routes</td><td>(Optional) Displays all the routes advertised to this neighbor.</td></tr><tr><td>flap-statistics</td><td>(Optional) Displays flap statistics for the routes received from this neighbor.</td></tr><tr><td>paths</td><td>(Optional) Displays AS paths learned from this neighbor.</td></tr><tr><td>received-routes</td><td>(Optional) Displays all the routes received from this neighbor.</td></tr><tr><td>routes</td><td>(Optional) Displays the routes received or advertised to or from this neighbor.</td></tr><tr><td>advertised</td><td>(Optional) Displays all the routes advertised for this neighbor.</td></tr><tr><td>dampened</td><td>(Optional) Displays all dampened routes received from this neighbor.</td></tr><tr><td>received</td><td>(Optional) Displays all the routes received from this neighbor.</td></tr><tr><td>prefix</td><td>(Optional) IPv6 prefix. The format is x.x.x.x/length.</td></tr><tr><td>vrf vrf-name</td><td>(Optional) Specifies the virtual router context (VRF) name. The name can be any case-sensitive, alphanumeric string up to 63 characters.</td></tr><tr><td>all</td><td>(Optional) Specifies all VRF.</td></tr></table>	Syntax	Description	addr	IPv4 address. The format is x.x.x.x.	advertised-routes	(Optional) Displays all the routes advertised to this neighbor.	flap-statistics	(Optional) Displays flap statistics for the routes received from this neighbor.	paths	(Optional) Displays AS paths learned from this neighbor.	received-routes	(Optional) Displays all the routes received from this neighbor.	routes	(Optional) Displays the routes received or advertised to or from this neighbor.	advertised	(Optional) Displays all the routes advertised for this neighbor.	dampened	(Optional) Displays all dampened routes received from this neighbor.	received	(Optional) Displays all the routes received from this neighbor.	prefix	(Optional) IPv6 prefix. The format is x.x.x.x/length.	vrf vrf-name	(Optional) Specifies the virtual router context (VRF) name. The name can be any case-sensitive, alphanumeric string up to 63 characters.	all	(Optional) Specifies all VRF.	<div>show ip bgp neighbors</div> <div>The show ip bgp neighbors command displays Border Gateway Protocol (BGP) and TCP session data for a specified IPv4 BGP neighbor, or for all IPv4 BGP neighbors if an address is not included.</div> <div>Platform all Command Mode EXEC</div> <div>Command Syntax</div> <div>show ip bgp neighbors [NEIGHBOR] [ADDR] [VRF] [INSTANCE]</div> <div>Parameters</div> <div><ul style="list-style-type: none">NEIGHBOR_ADDR location of neighbors. Options include:<ul style="list-style-type: none"><no parameter> command displays information for all IPv4 BGP neighbors.ipv4 addr command displays information for specified neighbor.VRF_INSTANCE specifies VRF instances.<ul style="list-style-type: none"><no parameter> displays routing table for context-active VRF.vrf vrf name displays routing table for the specified VRF.vrf all displays routing table for all VRFs.vrf default displays routing table for default VRF.</div>
Syntax	Description																											
addr	IPv4 address. The format is x.x.x.x.																											
advertised-routes	(Optional) Displays all the routes advertised to this neighbor.																											
flap-statistics	(Optional) Displays flap statistics for the routes received from this neighbor.																											
paths	(Optional) Displays AS paths learned from this neighbor.																											
received-routes	(Optional) Displays all the routes received from this neighbor.																											
routes	(Optional) Displays the routes received or advertised to or from this neighbor.																											
advertised	(Optional) Displays all the routes advertised for this neighbor.																											
dampened	(Optional) Displays all dampened routes received from this neighbor.																											
received	(Optional) Displays all the routes received from this neighbor.																											
prefix	(Optional) IPv6 prefix. The format is x.x.x.x/length.																											
vrf vrf-name	(Optional) Specifies the virtual router context (VRF) name. The name can be any case-sensitive, alphanumeric string up to 63 characters.																											
all	(Optional) Specifies all VRF.																											
Cisco NX-OS 5.0	Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 5.x (2010), at L3-686.	Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1632.																										
Effective date of registration: 11/13/2014		See also Arista User Manual v. 4.12.3 (7/17/13), at 1402; Arista User Manual, v. 4.11.1 (1/11/13), at 1148; Arista User Manual v. 4.10.3 (10/22/12), at 959.																										

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>Use the <code>ip ospf database</code> command to display information about different OSPF LSAs.</p> <p>When the link state advertisement is describing a network, the <i>link-state-id</i> argument can take one of two forms:</p> <ul style="list-style-type: none"> • The network's IP address (such as Type 3 summary link advertisements and autonomous system external link advertisements). • A derived address obtained from the link state ID. (Note that masking a network links advertisement's link state ID with the network's subnet mask yields the network's IP address.) • When the link state advertisement is describing a router, the link state ID is always the described router's OSPF router ID. • When an autonomous system external advertisement (LS Type = 5) is describing a default route, its link state ID is set to Default Destination (0.0.0.0). <p>This command requires the Enterprise Services license.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference (2013), at 520.</p>	<ul style="list-style-type: none"> • <i>linkstate_id</i> Network segment described by the LSA (dotted decimal notation). Value depends on the LSA type. <ul style="list-style-type: none"> — When the LSA describes a network, the <i>linkstate-id</i> argument is one of the following: <ul style="list-style-type: none"> The network IP address, as in Type 3 summary link advertisements and in autonomous system external link advertisements. A derived address obtained from the link state ID. Masking a network links the advertisement link state ID with the network subnet mask yielding the network IP address. — When the LSA describes a router, the link state ID is the OSPFv2 router ID of the router. — When an autonomous system external advertisement (Type 5) describes a default route, its link state ID is set to the default destination (0.0.0.0). <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1454.</p> <p><i>See also</i> Arista User Manual v. 4.13.6F (4/14/2014), at 1404; Arista User Manual v. 4.12.3 (7/17/13), at 1240; Arista User Manual, v. 4.11.1 (1/11/13), at 996; Arista User Manual v. 4.10.3 (10/22/12), at 825; Arista User Manual v. 4.9.3.2 (5/3/12), at 648; Arista User Manual v. 4.8.2 at 483; Arista User Manual v. 4.7.3 (7/18/11), at 357; Arista User Manual v. 4.6.0 (12/22/2010), at 217</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 5.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>Use the <code>ip ospf database</code> command to display information about different OSPF LSAs.</p> <p>When the link state advertisement is describing a network, the <i>link-state-id</i> argument can take one of two forms:</p> <ul style="list-style-type: none"> • The network's IP address (such as Type 3 summary link advertisements and autonomous system external link advertisements). • A derived address obtained from the link state ID. (Note that masking a network links advertisement's link state ID with the network's subnet mask yields the network's IP address.) • When the link state advertisement is describing a router, the link state ID is always the described router's OSPF router ID. • When an autonomous system external advertisement (LS Type = 5) is describing a default route, its link state ID is set to Default Destination (0.0.0.0). <p>This command requires the Enterprise Services license.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 5.x (2010), at L3-742.</p>	<ul style="list-style-type: none"> • <i>linkstate_id</i> Network segment described by the LSA (dotted decimal notation). Value depends on the LSA type. <ul style="list-style-type: none"> — When the LSA describes a network, the <i>linkstate-id</i> argument is one of the following: <ul style="list-style-type: none"> The network IP address, as in Type 3 summary link advertisements and in autonomous system external link advertisements. A derived address obtained from the link state ID. Masking a network links the advertisement link state ID with the network subnet mask yielding the network IP address. — When the LSA describes a router, the link state ID is the OSPFv2 router ID of the router. — When an autonomous system external advertisement (Type 5) describes a default route, its link state ID is set to the default destination (0.0.0.0). <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1454.</p> <p><i>See also</i> Arista User Manual v. 4.13.6F (4/14/2014), at 1404; Arista User Manual v. 4.12.3 (7/17/13), at 1240; Arista User Manual, v. 4.11.1 (1/11/13), at 996; Arista User Manual v. 4.10.3 (10/22/12), at 825; Arista User Manual v. 4.9.3.2 (5/3/12), at 648; Arista User Manual v. 4.8.2 at 483; Arista User Manual v. 4.7.3 (7/18/11), at 357; Arista User Manual v. 4.6.0 (12/22/2010), at 217</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 4.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>Use the <code>ip ospf database</code> command to display information about different OSPF LSAs.</p> <p>When the link state advertisement is describing a network, the <i>link-state-id</i> argument can take one of two forms:</p> <ul style="list-style-type: none"> • The network's IP address (such as Type 3 summary link advertisements and autonomous system external link advertisements). • A derived address obtained from the link state ID. (Note that masking a network links advertisement's link state ID with the network's subnet mask yields the network's IP address.) • When the link state advertisement is describing a router, the link state ID is always the described router's OSPF router ID. • When an autonomous system external advertisement (LS Type = 5) is describing a default route, its link state ID is set to Default Destination (0.0.0.0). <p>This command requires the Enterprise Services license.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 4.x (2008), at L3-426.</p>	<ul style="list-style-type: none"> • <i>linkstate_id</i> Network segment described by the LSA (dotted decimal notation). Value depends on the LSA type. <ul style="list-style-type: none"> — When the LSA describes a network, the <i>linkstate-id</i> argument is one of the following: <ul style="list-style-type: none"> • The network IP address, as in Type 3 summary link advertisements and in autonomous system external link advertisements. • A derived address obtained from the link state ID. Masking a network links the advertisement link state ID with the network subnet mask yielding the network IP address. — When the LSA describes a router, the link state ID is the OSPFv2 router ID of the router. — When an autonomous system external advertisement (Type 5) describes a default route, its link state ID is set to the default destination (0.0.0.0). <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1454.</p> <p><i>See also</i> Arista User Manual v. 4.13.6F (4/14/2014), at 1404; Arista User Manual v. 4.12.3 (7/17/13), at 1240; Arista User Manual, v. 4.11.1 (1/11/13), at 996; Arista User Manual v. 4.10.3 (10/22/12), at 825; Arista User Manual v. 4.9.3.2 (5/3/12), at 648; Arista User Manual v. 4.8.2 at 483; Arista User Manual v. 4.7.3 (7/18/11), at 357; Arista User Manual v. 4.6.0 (12/22/2010), at 217</p>

Copyright Registration Information	Cisco	Arista																								
<div>Cisco NX-OS 6.2</div> <div>Effective date of registration: 11/13/2014</div>	<div><div>timers lsa-arrival (OSPF)</div><div><div>To set the minimum interval in which the software accepts the same link-state advertisement (LSA) from Open Shortest Path First (OSPF) neighbors, use the timers lsa-arrival command. To return to the default, use the no form of this command.</div><div><div>timers lsa-arrival milliseconds</div><div>no timers lsa-arrival</div></div></div><table><tr><td>Syntax Description</td><td>milliseconds</td><td>Minimum delay (in milliseconds) that must pass between acceptance of the same LSA arriving from neighbors. The range is from 10 to 600,000 milliseconds. The default is 1000 milliseconds.</td></tr><tr><td>Defaults</td><td colspan="2">1000 milliseconds</td></tr><tr><td>Command Modes</td><td colspan="2">Router configuration VRF configuration</td></tr><tr><td>Supported User Roles</td><td colspan="2">network-admin vdc-admin</td></tr><tr><td>Command History</td><td>Release</td><td>Modification</td></tr><tr><td></td><td>4.0(1)</td><td>This command was introduced.</td></tr><tr><td>Usage Guidelines</td><td colspan="2"><div>Use the timers lsa arrival command to configure the minimum interval for accepting the same LSA. The same LSA is an LSA instance that contains the same LSA ID number, LSA type, and advertising router ID. If an instance of the same LSA arrives sooner than the interval that is set, the software drops the LSA.</div><div>We recommend that you keep the milliseconds value of the timers lsa-arrival command less than or equal to the neighbors' hold-interval value of the timers throttle lsa command.</div><div>This command requires the Enterprise Services license.</div></td></tr><tr><td>Examples</td><td colspan="2"><div>This example shows how to set the minimum interval for accepting the same LSA at 2000 milliseconds:</div><div>switch(config)# router ospf 1 switch(config-router)# timers lsa-arrival 2000</div></td></tr></table><div>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference (2013), at 1016.</div></div>	Syntax Description	milliseconds	Minimum delay (in milliseconds) that must pass between acceptance of the same LSA arriving from neighbors. The range is from 10 to 600,000 milliseconds. The default is 1000 milliseconds.	Defaults	1000 milliseconds		Command Modes	Router configuration VRF configuration		Supported User Roles	network-admin vdc-admin		Command History	Release	Modification		4.0(1)	This command was introduced.	Usage Guidelines	<div>Use the timers lsa arrival command to configure the minimum interval for accepting the same LSA. The same LSA is an LSA instance that contains the same LSA ID number, LSA type, and advertising router ID. If an instance of the same LSA arrives sooner than the interval that is set, the software drops the LSA.</div> <div>We recommend that you keep the milliseconds value of the timers lsa-arrival command less than or equal to the neighbors' hold-interval value of the timers throttle lsa command.</div> <div>This command requires the Enterprise Services license.</div>		Examples	<div>This example shows how to set the minimum interval for accepting the same LSA at 2000 milliseconds:</div> <div>switch(config)# router ospf 1 switch(config-router)# timers lsa-arrival 2000</div>		<div><div>timers lsa arrival (OSPFv2)</div><div><div>The timers lsa arrival command sets the minimum interval in which the switch accepts the same link-state advertisement (LSA) from OSPF neighbors.</div><div>The no timers lsa arrival and default timers lsa arrival commands restore the default maximum OSPFv2 path calculation interval to five seconds by removing the timers lsa arrival command from running-config.</div><div><div>Platformall</div><div>Command ModeRouter-OSPF Configuration</div></div><div><div>Command Syntax</div><div><div>timers lsa arrival lsa_time</div><div>no timers lsa arrival</div><div>default timers lsa arrival</div></div><div><div>Parameters</div><div><div>lsa_time</div><div>OSPFv2 minimum interval (seconds). Values range from 1 to 600000 milliseconds. Default is 1000 milliseconds.</div></div><div><div>Example</div><div><div>This command sets the minimum interval timer to ten milliseconds.</div><div><div>switch(config)#router ospf 6</div><div>switch(config-router-ospf)#timers lsa arrival 10</div><div>switch(config-router-ospf)#</div></div></div></div><div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1469.</div></div></div></div></div>
	Syntax Description	milliseconds	Minimum delay (in milliseconds) that must pass between acceptance of the same LSA arriving from neighbors. The range is from 10 to 600,000 milliseconds. The default is 1000 milliseconds.																							
Defaults	1000 milliseconds																									
Command Modes	Router configuration VRF configuration																									
Supported User Roles	network-admin vdc-admin																									
Command History	Release	Modification																								
	4.0(1)	This command was introduced.																								
Usage Guidelines	<div>Use the timers lsa arrival command to configure the minimum interval for accepting the same LSA. The same LSA is an LSA instance that contains the same LSA ID number, LSA type, and advertising router ID. If an instance of the same LSA arrives sooner than the interval that is set, the software drops the LSA.</div> <div>We recommend that you keep the milliseconds value of the timers lsa-arrival command less than or equal to the neighbors' hold-interval value of the timers throttle lsa command.</div> <div>This command requires the Enterprise Services license.</div>																									
Examples	<div>This example shows how to set the minimum interval for accepting the same LSA at 2000 milliseconds:</div> <div>switch(config)# router ospf 1 switch(config-router)# timers lsa-arrival 2000</div>																									

Copyright Registration Information	Cisco	Arista																								
<div>Cisco NX-OS 4.0</div> <div>Effective date of registration: 11/13/2014</div>	<div><div>timers lsa-arrival (OSPF)</div><div><div>To set the minimum interval in which the software accepts the same link-state advertisement (LSA) from Open Shortest Path First (OSPF) neighbors, use the timers lsa-arrival command. To return to the default, use the no form of this command.</div><div><div>timers lsa-arrival milliseconds</div><div>no timers lsa-arrival</div></div></div><table><tr><td>Syntax Description</td><td>milliseconds</td><td>Minimum delay (in milliseconds) that must pass between acceptance of the same LSA arriving from neighbors. The range is from 10 to 600,000 milliseconds. The default is 1000 milliseconds.</td></tr><tr><td>Defaults</td><td colspan="2">1000 milliseconds</td></tr><tr><td>Command Modes</td><td colspan="2">Router configuration VRF configuration</td></tr><tr><td>Supported User Roles</td><td colspan="2">network-admin vdc-admin</td></tr><tr><td>Command History</td><td>Release</td><td>Modification</td></tr><tr><td></td><td>4.0(1)</td><td>This command was introduced.</td></tr><tr><td>Usage Guidelines</td><td colspan="2"><div>Use the timers lsa arrival command to configure the minimum interval for accepting the same LSA. The same LSA is an LSA instance that contains the same LSA ID number, LSA type, and advertising router ID. If an instance of the same LSA arrives sooner than the interval that is set, the software drops the LSA.</div><div>We recommend that you keep the milliseconds value of the timers lsa-arrival command less than or equal to the neighbors' hold-interval value of the timers throttle lsa command.</div><div>This command requires the Enterprise Services license.</div></td></tr><tr><td>Examples</td><td colspan="2"><div>This example shows how to set the minimum interval for accepting the same LSA at 2000 milliseconds:</div><div>switch(config)# router ospf 1 switch(config-router)# timers lsa-arrival 2000</div></td></tr></table><div>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 4.x (2008), at L-540.</div></div>	Syntax Description	milliseconds	Minimum delay (in milliseconds) that must pass between acceptance of the same LSA arriving from neighbors. The range is from 10 to 600,000 milliseconds. The default is 1000 milliseconds.	Defaults	1000 milliseconds		Command Modes	Router configuration VRF configuration		Supported User Roles	network-admin vdc-admin		Command History	Release	Modification		4.0(1)	This command was introduced.	Usage Guidelines	<div>Use the timers lsa arrival command to configure the minimum interval for accepting the same LSA. The same LSA is an LSA instance that contains the same LSA ID number, LSA type, and advertising router ID. If an instance of the same LSA arrives sooner than the interval that is set, the software drops the LSA.</div> <div>We recommend that you keep the milliseconds value of the timers lsa-arrival command less than or equal to the neighbors' hold-interval value of the timers throttle lsa command.</div> <div>This command requires the Enterprise Services license.</div>		Examples	<div>This example shows how to set the minimum interval for accepting the same LSA at 2000 milliseconds:</div> <div>switch(config)# router ospf 1 switch(config-router)# timers lsa-arrival 2000</div>		<div><div>timers lsa arrival (OSPFv2)</div><div><div>The timers lsa arrival command sets the minimum interval in which the switch accepts the same link-state advertisement (LSA) from OSPF neighbors.</div><div>The no timers lsa arrival and default timers lsa arrival commands restore the default maximum OSPFv2 path calculation interval to five seconds by removing the timers lsa arrival command from running-config.</div><div><div>Platformall</div><div>Command ModeRouter-OSPF Configuration</div></div><div><div>Command Syntax</div><div>timers lsa arrival lsa_time no timers lsa arrival default timers lsa arrival</div></div><div><div>Parameters</div><div><div>lsa_time</div><div>OSPFv2 minimum interval (seconds). Values range from 1 to 600000 milliseconds. Default is 1000 milliseconds.</div></div></div><div><div>Example</div><div><div>This command sets the minimum interval timer to ten milliseconds.</div><div>switch(config)#router ospf 6 switch(config-router-ospf)#timers lsa arrival 10 switch(config-router-ospf)#</div></div></div><div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1469.</div></div></div>
	Syntax Description	milliseconds	Minimum delay (in milliseconds) that must pass between acceptance of the same LSA arriving from neighbors. The range is from 10 to 600,000 milliseconds. The default is 1000 milliseconds.																							
Defaults	1000 milliseconds																									
Command Modes	Router configuration VRF configuration																									
Supported User Roles	network-admin vdc-admin																									
Command History	Release	Modification																								
	4.0(1)	This command was introduced.																								
Usage Guidelines	<div>Use the timers lsa arrival command to configure the minimum interval for accepting the same LSA. The same LSA is an LSA instance that contains the same LSA ID number, LSA type, and advertising router ID. If an instance of the same LSA arrives sooner than the interval that is set, the software drops the LSA.</div> <div>We recommend that you keep the milliseconds value of the timers lsa-arrival command less than or equal to the neighbors' hold-interval value of the timers throttle lsa command.</div> <div>This command requires the Enterprise Services license.</div>																									
Examples	<div>This example shows how to set the minimum interval for accepting the same LSA at 2000 milliseconds:</div> <div>switch(config)# router ospf 1 switch(config-router)# timers lsa-arrival 2000</div>																									

Copyright Registration Information	Cisco	Arista																								
<div>Cisco NX-OS 5.0</div> <div>Effective date of registration: 11/13/2014</div>	<div><div>timers lsa-arrival (OSPF)</div><div><div>To set the minimum interval in which the software accepts the same link-state advertisement (LSA) from Open Shortest Path First (OSPF) neighbors, use the timers lsa-arrival command. To return to the default, use the no form of this command.</div><div><div>timers lsa-arrival milliseconds</div><div>no timers lsa-arrival</div></div></div><table><tr><td>Syntax Description</td><td>milliseconds</td><td>Minimum delay (in milliseconds) that must pass between acceptance of the same LSA arriving from neighbors. The range is from 10 to 600,000 milliseconds. The default is 1000 milliseconds.</td></tr><tr><td>Defaults</td><td colspan="2">1000 milliseconds</td></tr><tr><td>Command Modes</td><td colspan="2">Router configuration VRF configuration</td></tr><tr><td>Supported User Roles</td><td colspan="2">network-admin vdc-admin</td></tr><tr><td>Command History</td><td>Release</td><td>Modification</td></tr><tr><td></td><td>4.0(1)</td><td>This command was introduced.</td></tr><tr><td>Usage Guidelines</td><td colspan="2"><div>Use the timers lsa arrival command to configure the minimum interval for accepting the same LSA. The same LSA is an LSA instance that contains the same LSA ID number, LSA type, and advertising router ID. If an instance of the same LSA arrives sooner than the interval that is set, the software drops the LSA.</div><div>We recommend that you keep the milliseconds value of the timers lsa-arrival command less than or equal to the neighbors' hold-interval value of the timers throttle lsa command.</div><div>This command requires the Enterprise Services license.</div></td></tr><tr><td>Examples</td><td colspan="2"><div>This example shows how to set the minimum interval for accepting the same LSA at 2000 milliseconds:</div><div>switch(config)# router ospf 1 switch(config-router)# timers lsa-arrival 2000</div></td></tr></table><div>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 5.x (2010), at L-954.</div></div>	Syntax Description	milliseconds	Minimum delay (in milliseconds) that must pass between acceptance of the same LSA arriving from neighbors. The range is from 10 to 600,000 milliseconds. The default is 1000 milliseconds.	Defaults	1000 milliseconds		Command Modes	Router configuration VRF configuration		Supported User Roles	network-admin vdc-admin		Command History	Release	Modification		4.0(1)	This command was introduced.	Usage Guidelines	<div>Use the timers lsa arrival command to configure the minimum interval for accepting the same LSA. The same LSA is an LSA instance that contains the same LSA ID number, LSA type, and advertising router ID. If an instance of the same LSA arrives sooner than the interval that is set, the software drops the LSA.</div> <div>We recommend that you keep the milliseconds value of the timers lsa-arrival command less than or equal to the neighbors' hold-interval value of the timers throttle lsa command.</div> <div>This command requires the Enterprise Services license.</div>		Examples	<div>This example shows how to set the minimum interval for accepting the same LSA at 2000 milliseconds:</div> <div>switch(config)# router ospf 1 switch(config-router)# timers lsa-arrival 2000</div>		<div><div>timers lsa arrival (OSPFv2)</div><div><div>The timers lsa arrival command sets the minimum interval in which the switch accepts the same link-state advertisement (LSA) from OSPF neighbors.</div><div>The no timers lsa arrival and default timers lsa arrival commands restore the default maximum OSPFv2 path calculation interval to five seconds by removing the timers lsa arrival command from running-config.</div><div><div>Platformall</div><div>Command ModeRouter-OSPF Configuration</div></div><div><div>Command Syntax</div><div><div>timers lsa arrival lsa_time</div><div>no timers lsa arrival</div><div>default timers lsa arrival</div></div><div><div>Parameters</div><div><div>lsa_time</div><div>OSPFv2 minimum interval (seconds). Values range from 1 to 600000 milliseconds. Default is 1000 milliseconds.</div></div><div><div>Example</div><div><div>This command sets the minimum interval timer to ten milliseconds.</div><div><div>switch(config)#router ospf 6</div><div>switch(config-router-ospf)#timers lsa arrival 10</div><div>switch(config-router-ospf)#</div></div></div></div><div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1469.</div></div></div></div></div>
	Syntax Description	milliseconds	Minimum delay (in milliseconds) that must pass between acceptance of the same LSA arriving from neighbors. The range is from 10 to 600,000 milliseconds. The default is 1000 milliseconds.																							
Defaults	1000 milliseconds																									
Command Modes	Router configuration VRF configuration																									
Supported User Roles	network-admin vdc-admin																									
Command History	Release	Modification																								
	4.0(1)	This command was introduced.																								
Usage Guidelines	<div>Use the timers lsa arrival command to configure the minimum interval for accepting the same LSA. The same LSA is an LSA instance that contains the same LSA ID number, LSA type, and advertising router ID. If an instance of the same LSA arrives sooner than the interval that is set, the software drops the LSA.</div> <div>We recommend that you keep the milliseconds value of the timers lsa-arrival command less than or equal to the neighbors' hold-interval value of the timers throttle lsa command.</div> <div>This command requires the Enterprise Services license.</div>																									
Examples	<div>This example shows how to set the minimum interval for accepting the same LSA at 2000 milliseconds:</div> <div>switch(config)# router ospf 1 switch(config-router)# timers lsa-arrival 2000</div>																									

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>Examples</p> <p>This example shows how to configure a router configured with the start, hold, and maximum interval values for the <code>timers throttle spf</code> command set at 5, 1000, and 90,000 milliseconds:</p> <pre>switch(config)# router ospf 1 switch(config-router)# timers throttle spf 5 1000 90000</pre> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference (2013), at 1033-34.</p>	<p>Example</p> <ul style="list-style-type: none"> This command displays a switch configured with the start, hold, and maximum interval values for the <code>timers throttle spf</code> command set at 5, 1,000, and 20,000 milliseconds, respectively. <pre>switch(config)#router ospf 6 switch(config-router-ospf)#timers spf 5 100 20000 switch(config-router-ospf)#</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1472.</p>
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>When using route reflectors, an AS is divided into clusters. A cluster consists of one or more route reflectors and a group of clients to which they re-advertise route information. Multiple route reflectors can be configured in the same cluster to increase redundancy and avoid a single point of failure. Each route reflector has a cluster ID. If the cluster has a single route reflector, the cluster ID is its router ID. If a cluster has multiple route reflectors, a 4-byte cluster ID is assigned to all route reflectors in the cluster. All of them must be configured with the same cluster ID so that they can recognize updates from other route reflectors in the same cluster. The <code>bgp cluster-id</code> command configures the cluster ID in a cluster with multiple route reflectors.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference (2013), at 730.</p>	<p><code>cluster-id {cluster-id cluster-ip-addr}</code>—Configures the Route Reflector Cluster-ID (router, vrf). Range: 1 to 4294967295. You can enter the cluster identification as a 32-bit quantity or as an IP address. To remove the cluster ID, use the <code>no</code> form of this command. Together, a route reflector and its clients form a cluster. When a single route reflector is deployed in a cluster, the cluster is identified by the router ID of the route reflector.</p> <p>The <code>cluster-id</code> command is used to assign a cluster ID to a route reflector when the cluster has one or more route reflectors. Multiple route reflectors are deployed in a cluster to increase redundancy and avoid a single point of failure. When multiple route reflectors are configured in a cluster, the same cluster ID is assigned to all route reflectors. This allows all route reflectors in the cluster to recognize updates from peers in the same cluster and reduces the number of updates that need to be stored in BGP routing tables.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1549.</p>
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>Local Proxy ARP</p> <p>You can use local Proxy ARP to enable a device to respond to ARP requests for IP addresses within a subnet where normally no routing is required. When you enable local Proxy ARP, ARP responds to all ARP requests for IP addresses within the subnet and forwards all traffic between hosts in the subnet. Use this feature only on subnets where hosts are intentionally prevented from communicating directly by the configuration on the device to which they are connected.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 6.x (2013), at 2-5.</p>	<p>ip local-proxy-arp</p> <p>The <code>ip local-proxy-arp</code> command enables local proxy ARP (Address Resolution Protocol) on the configuration mode interface. Local proxy ARP programs the switch to respond to ARP requests for IP addresses within a subnet where routing is not normally required. A typical local proxy arp application is supporting isolated private VLANs that communicate with each other by routing packets.</p> <p>The <code>no ip local-proxy-arp</code> and default <code>ip local-proxy-arp</code> commands disable local proxy ARP on the configuration mode interface by removing the corresponding <code>ip local-proxy-arp</code> command from <code>running-config</code>.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1276.</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 1231; Arista User Manual v. 4.12.3 (7/17/13), at 1073; Arista User Manual, v. 4.11.1 (1/11/13), at 876; Arista User Manual v. 4.10.3 (10/22/12), at 707.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 5.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>Local Proxy ARP</p> <p>You can use local Proxy ARP to enable a device to respond to ARP requests for IP addresses within a subnet where normally no routing is required. When you enable local Proxy ARP, ARP responds to all ARP requests for IP addresses within the subnet and forwards all traffic between hosts in the subnet. Use this feature only on subnets where hosts are intentionally prevented from communicating directly by the configuration on the device to which they are connected.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x (2010), at 2-5.</p>	<p>ip local-proxy-arp</p> <p>The <code>ip local-proxy-arp</code> command enables local proxy ARP (Address Resolution Protocol) on the configuration mode interface. Local proxy ARP programs the switch to respond to ARP requests for IP addresses within a subnet where routing is not normally required. A typical local proxy arp application is supporting isolated private VLANs that communicate with each other by routing packets.</p> <p>The <code>no ip local-proxy-arp</code> and default <code>ip local-proxy-arp</code> commands disable local proxy ARP on the configuration mode interface by removing the corresponding <code>ip local-proxy-arp</code> command from <i>running-config</i>.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1276.</p> <p><i>See also</i> Arista User Manual v. 4.13.6F (4/14/2014), at 1231; Arista User Manual v. 4.12.3 (7/17/13), at 1073; Arista User Manual, v. 4.11.1 (1/11/13), at 876; Arista User Manual v. 4.10.3 (10/22/12), at 707.</p>
<p>Cisco NX-OS 4.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>Local Proxy ARP</p> <p>You can use local Proxy ARP to enable a device to respond to ARP requests for IP addresses within a subnet where normally no routing is required. When you enable local Proxy ARP, ARP responds to all ARP requests for IP addresses within the subnet and forwards all traffic between hosts in the subnet. Use this feature only on subnets where hosts are intentionally prevented from communicating directly by the configuration on the device to which they are connected.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 4.0 (2008), at 2-5.</p>	<p>ip local-proxy-arp</p> <p>The <code>ip local-proxy-arp</code> command enables local proxy ARP (Address Resolution Protocol) on the configuration mode interface. Local proxy ARP programs the switch to respond to ARP requests for IP addresses within a subnet where routing is not normally required. A typical local proxy arp application is supporting isolated private VLANs that communicate with each other by routing packets.</p> <p>The <code>no ip local-proxy-arp</code> and default <code>ip local-proxy-arp</code> commands disable local proxy ARP on the configuration mode interface by removing the corresponding <code>ip local-proxy-arp</code> command from <i>running-config</i>.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1276.</p> <p><i>See also</i> Arista User Manual v. 4.13.6F (4/14/2014), at 1231; Arista User Manual v. 4.12.3 (7/17/13), at 1073; Arista User Manual, v. 4.11.1 (1/11/13), at 876; Arista User Manual v. 4.10.3 (10/22/12), at 707.</p>

Copyright Registration Information	Cisco		Arista
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	ipv6 nd managed-config-flag	Sets the managed address configuration flag in IPv6 router advertisements.	Router Advertisement Flag Configuration The <code>ipv6 nd managed-config-flag</code> command configures the switch to set the <i>managed address configuration</i> flag in IPv6 router advertisements transmitted from the configuration mode interface. This bit instructs receptive hosts to use stateful address autoconfiguration. The <code>ipv6 nd other-config-flag</code> command configures the switch to set the <i>other stateful configuration flag</i> in IPv6 router advertisements transmitted from the configuration mode interface. This flag indicates the availability of autoconfiguration information, other than addresses, and that hosts should use stateful Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1329. <i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1119; Arista User Manual, v. 4.11.1 (1/11/13), at 887; Arista User Manual v. 4.10.3 (10/22/12), at 733.
	ipv6 nd mtu	Sets the maximum transmission unit (MTU) size of IPv6 packets sent on an interface.	
	ipv6 nd ns-interval	Configures the interval between IPv6 neighbor solicitation retransmissions on an interface.	
	ipv6 nd other-config-flag	Configures the other stateful configuration flag in IPv6 router advertisements.	
Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 6.x (2013), at 3-24.			
Cisco NX-OS 5.x Effective date of registration: 11/13/2014	ipv6 nd managed-config-flag	Sets the managed address configuration flag in IPv6 router advertisements.	Router Advertisement Flag Configuration The <code>ipv6 nd managed-config-flag</code> command configures the switch to set the <i>managed address configuration</i> flag in IPv6 router advertisements transmitted from the configuration mode interface. This bit instructs receptive hosts to use stateful address autoconfiguration. The <code>ipv6 nd other-config-flag</code> command configures the switch to set the <i>other stateful configuration flag</i> in IPv6 router advertisements transmitted from the configuration mode interface. This flag indicates the availability of autoconfiguration information, other than addresses, and that hosts should use stateful Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1329. <i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1119; Arista User Manual, v. 4.11.1 (1/11/13), at 887; Arista User Manual v. 4.10.3 (10/22/12), at 733.
	ipv6 nd mtu	Sets the maximum transmission unit (MTU) size of IPv6 packets sent on an interface.	
	ipv6 nd ns-interval	Configures the interval between IPv6 neighbor solicitation retransmissions on an interface.	
	ipv6 nd other-config-flag	Configures the other stateful configuration flag in IPv6 router advertisements.	
Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x (2010), at 3-22.			

Copyright Registration Information	Cisco		Arista
Cisco NX-OS 4.0 Effective date of registration: 11/13/2014	ipv6 nd managed-config-flag	Sets the managed address configuration flag in IPv6 router advertisements.	Router Advertisement Flag Configuration The <code>ipv6 nd managed-config-flag</code> command configures the switch to set the <i>managed address configuration flag</i> in IPv6 router advertisements transmitted from the configuration mode interface. This bit instructs receptive hosts to use stateful address autoconfiguration. The <code>ipv6 nd other-config-flag</code> command configures the switch to set the <i>other stateful configuration flag</i> in IPv6 router advertisements transmitted from the configuration mode interface. This flag indicates the availability of autoconfiguration information, other than addresses, and that hosts should use stateful
	ipv6 nd mtu	Sets the maximum transmission unit (MTU) size of IPv6 packets sent on an interface.	
	ipv6 nd ns-interval	Configures the interval between IPv6 neighbor solicitation retransmissions on an interface.	
	ipv6 nd other-config-flag	Configures the other stateful configuration flag in IPv6 router advertisements.	
Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 4.0 (2008), at 3-22.		Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1329. <i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1119; Arista User Manual, v. 4.11.1 (1/11/13), at 887; Arista User Manual v. 4.10.3 (10/22/12), at 733.	
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	ipv6 nd reachable-time	Configures the amount of time that a remote IPv6 node is considered reachable after some reachability confirmation event has occurred.	ipv6 nd reachable-time The <code>ipv6 nd reachable-time</code> command specifies the time period that the switch includes in the reachable time field of Router Advertisements (RAs) sent from the configuration mode interface. The reachable time defines the period that a remote IPv6 node is considered reachable after a reachability confirmation event. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1359. <i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1149.
	Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 6.x (2013), at 3-24.		
Cisco NX-OS 5.0 Effective date of registration: 11/13/2014	ipv6 nd reachable-time	Configures the amount of time that a remote IPv6 node is considered reachable after some reachability confirmation event has occurred.	ipv6 nd reachable-time The <code>ipv6 nd reachable-time</code> command specifies the time period that the switch includes in the reachable time field of Router Advertisements (RAs) sent from the configuration mode interface. The reachable time defines the period that a remote IPv6 node is considered reachable after a reachability confirmation event. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1359. <i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1149.
	Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x (2010), at 3-22.		



Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 4.0</p> <p>Effective date of registration: 11/13/2014</p>	<p><u>ipv6 nd reachable-time</u></p> <hr/> <p>Configures the amount of time <u>that a remote IPv6 node is considered reachable after some reachability confirmation event</u> has occurred.</p> <hr/> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 4.0 (2008), at 3-22.</p>	<p>ipv6 nd reachable-time</p> <p>The <u>ipv6 nd reachable-time</u> command specifies the time period that the switch includes in the reachable time field of Router Advertisements (RAs) sent from the configuration mode interface. The reachable time defines the period <u>that a remote IPv6 node is considered reachable after a reachability confirmation event</u>.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1359.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1149.</p>


Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>Step 3 <code>max-metric router-lsa {external-lsa [max-metric-value]} [stub-prefix-lsa [on-startup [seconds] wait-for-bgp tag]] [inter-area-prefix-lsa [max-metric-sumlsa]]</code></p> <p>Example: <code>switch(config-router)# max-metric router-lsa on-startup wait-for-bgp</code></p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 6.x (2013), at 7-42.</p>	<p>max-metric router-lsa (OSPFv3)</p> <p>The <code>max-metric router-lsa</code> command allows the OSPFv3 protocol to advertise a maximum metric so that other routers do not prefer the router as an intermediate hop in their SPF calculations.</p> <p>The <code>no max-metric router-lsa</code> and <code>default max-metric router-lsa</code> commands disable the advertisement of a maximum metric.</p> <p>Platform all Command Mode Router-OSPF3 Configuration</p> <p>Command Syntax</p> <pre>max-metric router-lsa {EXTERNAL} {STUB} {STARTUP} {SUMMARY} no max-metric router-lsa {EXTERNAL} {STUB} {STARTUP} {SUMMARY} default max-metric router-lsa {EXTERNAL} {STUB} {STARTUP} {SUMMARY}</pre> <p>All parameters can be placed in any order.</p> <p>Parameters</p> <ul style="list-style-type: none"> EXTERNAL advertised metric value. Values include: <ul style="list-style-type: none"> <no parameter> Metric is set to the default value of 1. <code>external-lsa</code> Configures the router to override the External LSA / NSSA-External metric with the maximum metric value. <code>external-lsa <1 to 16777215></code> The configurable range is from 1 to 0xFFFFFFFF. The default value is 0xFFFF0000. This range can be used with external LSA, summary LSA extensions to indicate the respective metric you want with the LSA. STUB advertised metric type. Values include: <ul style="list-style-type: none"> <no parameter> Metric type is set to the default value of 2. <code>include-stub</code> Advertises stub links in router-LSA with the max-metric value (0xFFFF). STARTUP limit scope of LSAs. Values include: <ul style="list-style-type: none"> <no parameter> LSA can be translated <code>on-startup</code> Configures the router to advertise a maximum metric at startup (only valid in no and default command formats). <code>on-startup wait-for-bgp</code> Configures the router to advertise a maximum metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired. The default timer is 600 seconds. <code>on-startup <5 to 86400></code> Sets the maximum metric temporarily after a reboot to originate router-LSAs with the max-metric value. <p><code>wait-for-bgp</code> or an <code>on-start</code> time value is not included in no and default commands.</p> SUMMARY advertised metric value. Values include: <ul style="list-style-type: none"> <no parameter> Metric is set to the default value of 1. <code>summary-lsa</code> Configures the router to override the summary LSA metric with the maximum metric value for both type 3 and type 4 Summary LSAs. <code>summary-lsa <1 to 16777215></code> Metric is set to the specified value. <p>Example</p> <ul style="list-style-type: none"> This command shows how to configure OSPFv3 to originate router LSAs with the maximum metric until BGP indicates that it has converged: <pre>switch(config-router-ospf3)#max-metric router-lsa on-startup wait-for-bgp switch(config-router-ospf3)#</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1519.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>IS-IS Overview</p> <p>IS-IS sends a hello packet out every configured interface to discover IS-IS neighbor routers. The hello packet contains information, such as the authentication, area, and supported protocols, which the receiving interface uses to determine compatibility with the originating interface. The hello packets are also padded to ensure that IS-IS establishes adjacencies only with interfaces that have matching maximum transmission unit (MTU) settings. Compatible interfaces form adjacencies, which update routing information in the link-state database through link-state update messages (LSPs). By default, the router sends a periodic LSP refresh every 10 minutes and the LSPs remain in the link-state database for 20 minutes (the LSP lifetime). If the router does not receive an LSP refresh before the end of the LSP lifetime, the router deletes the LSP from the database.</p> <p>The LSP interval must be less than the LSP lifetime or the LSPs time out before they are refreshed.</p> <p>IS-IS sends periodic hello packets to adjacent routers. If you configure transient mode for hello packets, these hello packets do not include the excess padding used before IS-IS establishes adjacencies. If the MTU value on adjacent routers changes, IS-IS can detect this change and send padded hello packets for a period of time. IS-IS uses this feature to detect mismatched MTU values on adjacent routers. For more information, see the "Configuring the Transient Mode for Hello Padding" section on page 9-21.</p> <p>IS-IS Areas</p> <p>You can design IS-IS networks as a single area that includes all routers in the network or as multiple areas that connect into a backbone or Level 2 area. Routers in a nonbackbone area are Level 1 routers that establish adjacencies within a local area (intra-area routing). Level 2 area routers establish adjacencies to other Level 2 routers and perform routing between Level 1 areas (inter-area routing). A router can have both Level 1 and Level 2 areas configured. These Level 1/Level 2 routers act as area border routers that route information from the local area to the Level 2 backbone area (see Figure 9-1).</p> <p>Within a Level 1 area, routers know how to reach all other routers in that area. The Level 2 routers know how to reach other area border routers and other Level 2 routers. Level 1/Level 2 routers straddle the boundary between two areas, routing traffic to and from the Level 2 backbone area. Level 1/Level 2 routers use the attached (ATT) bit signal Level 1 routers to set a default route to this Level 1/Level 2 router to connect to the Level 2 area.</p> <p>In some instances, such as when you have two or more Level 1/Level 2 routers in an area, you may want to control which Level 1/Level 2 router that the Level 1 routers use as the default route to the Level 2 area. You can configure which Level 1/Level 2 router sets the attached bit. For more information, see the "Verifying the IS-IS Configuration" section on page 9-33.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 6.x (2013), at 9-2.</p>	<p>IS-IS Description</p> <p>IS-IS sends a hello packet out every configured interface to discover IS-IS neighbor routers. The hello packet contains information, which the receiving interface uses to determine compatibility with the originating interface. Compatible interfaces form adjacencies, which update routing information in the link-state database through link-state update messages (LSPs). If the router does not receive an LSP refresh before the end of the LSP lifetime, the device deletes the LSP from the database.</p> <p>Terms of IS-IS Routing Protocol</p> <p>The following terms are used when configuring IS-IS.</p> <ul style="list-style-type: none"> • NET and System ID – Each IS-IS instance has an associated network entity title (NET). The NET consists of the IS-IS system ID, which uniquely identifies the IS-IS instance in the area and the area ID. • Designated Intermediate System – IS-IS uses a Designated Intermediate System (DIS) in broadcast networks to prevent each device from forming unnecessary links with every other device on the broadcast network. IS-IS devices send LSPs to the DIS, which manages all the link-state information for the broadcast network. You can configure the IS-IS priority that IS-IS uses to select the DIS in an area. • IS-IS Areas – You can design IS-IS networks as a single area that includes all routers in the network or as multiple areas that connect into a backbone or Level 2 area. Routers in a nonbackbone area are Level 1 routers that establish adjacencies within a local area (intra-area routing). Level 2 area routers establish adjacencies to other Level 2 routers and perform routing between Level 1 areas (inter-area routing). A router can have both Level 1 and Level 2 areas configured. • IS-IS Instances – Arista supports only one instance of the IS-IS protocol that run on the same node. • LSP – Link state packet (LSP) can switch link state information. LSPs fall into two types: Level 1 LSPs and Level 2 LSPs. Level 2 devices transmit Level 2 LSPs; Level-1 devices transmit Level 1 LSPs; Level 1-2 devices transmit both Level 2 LSPs and Level 1 LSPs. • Hello packets – Hello packets, can establish and maintain neighbor relationships. • Overload Bit – IS-IS uses the overload bit to tell other devices not to use the local router to forward traffic but to continue routing traffic destined for that local router. Possible conditions for setting the overload bit the device is in a critical condition. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1674.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1436.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 5.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>IS-IS Overview</p> <p>IS-IS sends a hello packet out every configured interface to discover IS-IS neighbor routers. The hello packet contains information, such as the authentication, area, and supported protocols, which the receiving interface uses to determine compatibility with the originating interface. The hello packets are also padded to ensure that IS-IS establishes adjacencies only with interfaces that have matching maximum transmission unit (MTU) settings. Compatible interfaces form adjacencies, which update routing information in the link-state database through link-state update messages (LSPs). By default, the router sends a periodic LSP refresh every 10 minutes and the LSPs remain in the link-state database for 20 minutes (the LSP lifetime). If the router does not receive an LSP refresh before the end of the LSP lifetime, the router deletes the LSP from the database.</p> <p>The LSP interval must be less than the LSP lifetime or the LSPs time out before they are refreshed.</p> <p>IS-IS sends periodic hello packets to adjacent routers. If you configure transient mode for hello packets, these hello packets do not include the excess padding used before IS-IS establishes adjacencies. If the MTU value on adjacent routers changes, IS-IS can detect this change and send padded hello packets for a period of time. IS-IS uses this feature to detect mismatched MTU values on adjacent routers. For more information, see the "Configuring the Transient Mode for Hello Padding" section on page 9-21.</p> <p>IS-IS Areas</p> <p>You can design IS-IS networks as a single area that includes all routers in the network or as multiple areas that connect into a backbone or Level 2 area. Routers in a nonbackbone area are Level 1 routers that establish adjacencies within a local area (intra-area routing). Level 2 area routers establish adjacencies to other Level 2 routers and perform routing between Level 1 areas (inter-area routing). A router can have both Level 1 and Level 2 areas configured. These Level 1/Level 2 routers act as area border routers that route information from the local area to the Level 2 backbone area (see Figure 9-1).</p> <p>Within a Level 1 area, routers know how to reach all other routers in that area. The Level 2 routers know how to reach other area border routers and other Level 2 routers. Level 1/Level 2 routers straddle the boundary between two areas, routing traffic to and from the Level 2 backbone area. Level 1/Level 2 routers use the attached (ATT) bit signal Level 1 routers to set a default route to this Level 1/Level 2 router to connect to the Level 2 area.</p> <p>In some instances, such as when you have two or more Level 1/Level 2 routers in an area, you may want to control which Level 1/Level 2 router that the Level 1 routers use as the default route to the Level 2 area. You can configure which Level 1/Level 2 router sets the attached bit. For more information, see the "Verifying the IS-IS Configuration" section on page 9-33.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x (2010), at 9-2.</p>	<p>IS-IS Description</p> <p>IS-IS sends a hello packet out every configured interface to discover IS-IS neighbor routers. The hello packet contains information, which the receiving interface uses to determine compatibility with the originating interface. Compatible interfaces form adjacencies, which update routing information in the link-state database through link-state update messages (LSPs). If the router does not receive an LSP refresh before the end of the LSP lifetime, the device deletes the LSP from the database.</p> <p>Terms of IS-IS Routing Protocol</p> <p>The following terms are used when configuring IS-IS.</p> <ul style="list-style-type: none"> • NET and System ID – Each IS-IS instance has an associated network entity title (NET). The NET consists of the IS-IS system ID, which uniquely identifies the IS-IS instance in the area and the area ID. • Designated Intermediate System – IS-IS uses a Designated Intermediate System (DIS) in broadcast networks to prevent each device from forming unnecessary links with every other device on the broadcast network. IS-IS devices send LSPs to the DIS, which manages all the link-state information for the broadcast network. You can configure the IS-IS priority that IS-IS uses to select the DIS in an area. • IS-IS Areas – You can design IS-IS networks as a single area that includes all routers in the network or as multiple areas that connect into a backbone or Level 2 area. Routers in a nonbackbone area are Level 1 routers that establish adjacencies within a local area (intra-area routing). Level 2 area routers establish adjacencies to other Level 2 routers and perform routing between Level 1 areas (inter-area routing). A router can have both Level 1 and Level 2 areas configured. • IS-IS Instances – Arista supports only one instance of the IS-IS protocol that run on the same node. • LSP – Link state packet (LSP) can switch link state information. LSPs fall into two types: Level 1 LSPs and Level 2 LSPs. Level 2 devices transmit Level 2 LSPs; Level-1 devices transmit Level 1 LSPs; Level 1-2 devices transmit both Level 2 LSPs and Level 1 LSPs. • Hello packets – Hello packets, can establish and maintain neighbor relationships. • Overload Bit – IS-IS uses the overload bit to tell other devices not to use the local router to forward traffic but to continue routing traffic destined for that local router. Possible conditions for setting the overload bit the device is in a critical condition. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1674.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1436.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 4.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>IS-IS Overview</p> <p>IS-IS sends a hello packet out every configured interface to discover IS-IS neighbor routers. The hello packet contains information, such as the authentication, area, and supported protocols, which the receiving interface uses to determine compatibility with the originating interface. The hello packets are also padded to ensure that IS-IS establishes adjacencies only with interfaces that have matching maximum transmission unit (MTU) settings. Compatible interfaces form adjacencies, which update routing information in the link-state database through link-state update messages (LSPs). By default, the router sends a periodic LSP refresh every 10 minutes and the LSPs remain in the link-state database for 20 minutes (the LSP lifetime). If the router does not receive an LSP refresh before the end of the LSP lifetime, the router deletes the LSP from the database.</p> <p>The LSP interval must be less than the LSP lifetime or the LSPs time out before they are refreshed.</p> <p>IS-IS sends periodic hello packets to adjacent routers. If you configure transient mode for hello packets, these hello packets do not include the excess padding used before IS-IS establishes adjacencies. If the MTU value on adjacent routers changes, IS-IS can detect this change and send padded hello packets for a period of time. IS-IS uses this feature to detect mismatched MTU values on adjacent routers. For more information, see the "Configuring the Transient Mode for Hello Padding" section on page 9-21.</p> <p>IS-IS Areas</p> <p>You can design IS-IS networks as a single area that includes all routers in the network or as multiple areas that connect into a backbone or Level 2 area. Routers in a nonbackbone area are Level 1 routers that establish adjacencies within a local area (intra-area routing). Level 2 area routers establish adjacencies to other Level 2 routers and perform routing between Level 1 areas (inter-area routing). A router can have both Level 1 and Level 2 areas configured. These Level 1/Level 2 routers act as area border routers that route information from the local area to the Level 2 backbone area (see Figure 9-1).</p> <p>Within a Level 1 area, routers know how to reach all other routers in that area. The Level 2 routers know how to reach other area border routers and other Level 2 routers. Level 1/Level 2 routers straddle the boundary between two areas, routing traffic to and from the Level 2 backbone area. Level 1/Level 2 routers use the attached (ATT) bit signal Level 1 routers to set a default route to this Level 1/Level 2 router to connect to the Level 2 area.</p> <p>In some instances, such as when you have two or more Level 1/Level 2 routers in an area, you may want to control which Level 1/Level 2 router that the Level 1 routers use as the default route to the Level 2 area. You can configure which Level 1/Level 2 router sets the attached bit. For more information, see the "Verifying the IS-IS Configuration" section on page 9-33.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 4.0 (2008), at 8-2.</p>	<p>IS-IS Description</p> <p>IS-IS sends a hello packet out every configured interface to discover IS-IS neighbor routers. The hello packet contains information, which the receiving interface uses to determine compatibility with the originating interface. Compatible interfaces form adjacencies, which update routing information in the link-state database through link-state update messages (LSPs). If the router does not receive an LSP refresh before the end of the LSP lifetime, the device deletes the LSP from the database.</p> <p>Terms of IS-IS Routing Protocol</p> <p>The following terms are used when configuring IS-IS.</p> <ul style="list-style-type: none"> NET and System ID – Each IS-IS instance has an associated network entity title (NET). The NET consists of the IS-IS system ID, which uniquely identifies the IS-IS instance in the area and the area ID. Designated Intermediate System – IS-IS uses a Designated Intermediate System (DIS) in broadcast networks to prevent each device from forming unnecessary links with every other device on the broadcast network. IS-IS devices send LSPs to the DIS, which manages all the link-state information for the broadcast network. You can configure the IS-IS priority that IS-IS uses to select the DIS in an area. IS-IS Areas – You can design IS-IS networks as a single area that includes all routers in the network or as multiple areas that connect into a backbone or Level 2 area. Routers in a nonbackbone area are Level 1 routers that establish adjacencies within a local area (intra-area routing). Level 2 area routers establish adjacencies to other Level 2 routers and perform routing between Level 1 areas (inter-area routing). A router can have both Level 1 and Level 2 areas configured. IS-IS Instances – Arista supports only one instance of the IS-IS protocol that run on the same node. LSP – Link state packet (LSP) can switch link state information. LSPs fall into two types: Level 1 LSPs and Level 2 LSPs. Level 2 devices transmit Level 2 LSPs; Level-1 devices transmit Level 1 LSPs; Level 1-2 devices transmit both Level 2 LSPs and Level 1 LSPs. Hello packets – Hello packets, can establish and maintain neighbor relationships. Overload Bit – IS-IS uses the overload bit to tell other devices not to use the local router to forward traffic but to continue routing traffic destined for that local router. Possible conditions for setting the overload bit the device is in a critical condition. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1674.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1436.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>NET and System ID</p> <p>Each IS-IS instance has an associated network entity title (NET). The NET is comprised of the IS-IS system ID, which uniquely identifies this IS-IS instance in the area and the area ID. For example, if the NET is 47.0004.004d.0001.0001.0e11.1111.00, the system ID is 0000.0e11.1111.00 and the area is ID 47.0004.004d.0001.</p> <p>Designated Intermediate System</p> <p>IS-IS uses a designated intermediate system (DIS) in broadcast networks to prevent each router from forming unnecessary links with every other router on the broadcast network. IS-IS routers send LSPs to the DIS, which manages all the link-state information for the broadcast network. You can configure the IS-IS priority that IS-IS uses to select the DIS in an area.</p> <p> Note No DIS is required on a point-to-point network.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 6.x (2013), at 9-3.</p>	<p>Terms of IS-IS Routing Protocol</p> <p>The following terms are used when configuring IS-IS.</p> <ul style="list-style-type: none"> • NET and System ID – Each IS-IS instance has an associated network entity title (NET). The NET consists of the IS-IS system ID, which uniquely identifies the IS-IS instance in the area and the area ID. • Designated Intermediate System – IS-IS uses a Designated Intermediate System (DIS) in broadcast networks to prevent each device from forming unnecessary links with every other device on the broadcast network. IS-IS devices send LSPs to the DIS, which manages all the link-state information for the broadcast network. You can configure the IS-IS priority that IS-IS uses to select the DIS in an area. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1674.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1436.</p>
<p>Cisco NX-OS 5.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>NET and System ID</p> <p>Each IS-IS instance has an associated network entity title (NET). The NET is comprised of the IS-IS system ID, which uniquely identifies this IS-IS instance in the area and the area ID. For example, if the NET is 47.0004.004d.0001.0001.0e11.1111.00, the system ID is 0000.0e11.1111.00 and the area is ID 47.0004.004d.0001.</p> <p>Designated Intermediate System</p> <p>IS-IS uses a designated intermediate system (DIS) in broadcast networks to prevent each router from forming unnecessary links with every other router on the broadcast network. IS-IS routers send LSPs to the DIS, which manages all the link-state information for the broadcast network. You can configure the IS-IS priority that IS-IS uses to select the DIS in an area.</p> <p> Note No DIS is required on a point-to-point network.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x (2010), at 9-3.</p>	<p>Terms of IS-IS Routing Protocol</p> <p>The following terms are used when configuring IS-IS.</p> <ul style="list-style-type: none"> • NET and System ID – Each IS-IS instance has an associated network entity title (NET). The NET consists of the IS-IS system ID, which uniquely identifies the IS-IS instance in the area and the area ID. • Designated Intermediate System – IS-IS uses a Designated Intermediate System (DIS) in broadcast networks to prevent each device from forming unnecessary links with every other device on the broadcast network. IS-IS devices send LSPs to the DIS, which manages all the link-state information for the broadcast network. You can configure the IS-IS priority that IS-IS uses to select the DIS in an area. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1674.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1436.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 4.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>NET and System ID</p> <p>Each IS-IS instance has an associated network entity title (NET). The NET is comprised of the IS-IS system ID, which uniquely identifies this IS-IS instance in the area and the area ID. For example, if the NET is 47.0004.004d.0001.0001.0c11.1111.00, the system ID is 0000.0c11.1111.00 and the area is ID 47.0004.004d.0001.</p> <p>Designated Intermediate System</p> <p>IS-IS uses a designated intermediate system (DIS) in broadcast networks to prevent each router from forming unnecessary links with every other router on the broadcast network. IS-IS routers send LSPs to the DIS, which manages all the link-state information for the broadcast network. You can configure the IS-IS priority that IS-IS uses to select the DIS in an area.</p> <p> Note No DIS is required on a point-to-point network.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 4.0 (2008), at 8-3.</p>	<p>Terms of IS-IS Routing Protocol</p> <p>The following terms are used when configuring IS-IS.</p> <ul style="list-style-type: none"> NET and System ID – Each IS-IS instance has an associated network entity title (NET). The NET consists of the IS-IS system ID, which uniquely identifies the IS-IS instance in the area and the area ID. Designated Intermediate System – IS-IS uses a Designated Intermediate System (DIS) in broadcast networks to prevent each device from forming unnecessary links with every other device on the broadcast network. IS-IS devices send LSPs to the DIS, which manages all the link-state information for the broadcast network. You can configure the IS-IS priority that IS-IS uses to select the DIS in an area. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1674.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1436.</p>
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>Overload Bit</p> <p>IS-IS uses the overload bit to tell other routers not to use the local router to forward traffic but to continue routing traffic destined for that local router.</p> <p>You may want to use the overload bit in these situations:</p> <ul style="list-style-type: none"> The router is in a critical condition. Graceful introduction and removal of the router to/from the network. Other (administrative or traffic engineering) reasons such as waiting for BGP convergence. <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 6.x (2013), at 9-4.</p>	<ul style="list-style-type: none"> Overload Bit – IS-IS uses the overload bit to tell other devices not to use the local router to forward traffic but to continue routing traffic destined for that local router. Possible conditions for setting the overload bit the device is in a critical condition. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1674.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1436.</p>
<p>Cisco NX-OS 5.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>Overload Bit</p> <p>IS-IS uses the overload bit to tell other routers not to use the local router to forward traffic but to continue routing traffic destined for that local router.</p> <p>You may want to use the overload bit in these situations:</p> <ul style="list-style-type: none"> The router is in a critical condition. Graceful introduction and removal of the router to/from the network. Other (administrative or traffic engineering) reasons such as waiting for BGP convergence. <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x (2010), at 9-4.</p>	<ul style="list-style-type: none"> Overload Bit – IS-IS uses the overload bit to tell other devices not to use the local router to forward traffic but to continue routing traffic destined for that local router. Possible conditions for setting the overload bit the device is in a critical condition. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1674.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1436.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 4.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>Overload Bit</p> <p>IS-IS uses the overload bit to tell other routers not to use the local router to forward traffic but to continue routing traffic destined for that local router.</p> <p>You may want to use the overload bit in these situations:</p> <ul style="list-style-type: none"> The router is in a critical condition. Graceful introduction and removal of the router to/from the network. Other (administrative or traffic engineering) reasons such as waiting for BGP convergence. <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 4.0 (2008), at 8-4.</p>	<ul style="list-style-type: none"> Overload Bit – IS-IS uses the overload bit to tell other devices not to use the local router to forward traffic but to continue routing traffic destined for that local router. Possible conditions for setting the overload bit the device is in a critical condition. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1674.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1436.</p>

Copyright Registration Information	Cisco	Arista
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<div><div><pre>isis hello-multiplier num [level-1 level-2]</pre><p>Example: switch(config-if)# isis hello-multiplier 20</p></div><div>Specifies the number of IS-IS hello packets that a neighbor must miss before the router tears down an adjacency. The range is from 3 to 1000. The default is 3.</div></div> <div>Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 6.x (2013), at 9-33.</div>	<div><div>isis hello-multiplier</div><div>The isis hello-multiplier command specifies the number of IS-IS hello packets a neighbor must miss before the device should declare the adjacency as down.</div><div>Each hello packet contains a hold time. The hold time informs the receiving devices how long to wait without seeing another hello from the sending device before considering the sending device down. The isis hello-multiplier command is used to calculate the hold time announced in hello packets by multiplying this number with the configured isis hello-interval.</div><div>The no isis hello-multiplier and default isis hello-multiplier commands restore the default hello interval of 3 on the configuration mode interface by removing the isis hello-multiplier command from running-config.</div><div><div>Platform</div><div>all</div><div>Command Mode</div><div>Interface-Ethernet Configuration Interface-Loopback Configuration Interface-Port-channel Configuration Interface-VLAN Configuration</div></div><div>Command Syntax</div><div>isis hello-multiplier factor no isis hello-multiplier default isis hello-multiplier</div><div>Parameters</div><div><ul style="list-style-type: none">factor hello multiplier. Values range from 3 to 100; default is 3</div><div>Examples</div><div><ul style="list-style-type: none">These commands configure a hello multiplier of 4 for VLAN 200.<div>switch(config)#interface vlan 200 switch(config-if-V1200)#isis hello-multiplier 4 switch(config-if-V1200)#</div></div><div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1685.</div><div>See also Arista User Manual v. 4.12.3 (7/17/13), at 1447.</div></div>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>Step 9 <code>route-reflector-client</code></p> <p>example: <code>switch(config-router-neighbor-ar)# route-reflector-client</code></p> <p>Configures the device as a BGP route reflector and configures the neighbor as its client. This command triggers an automatic notification and session reset for the BGP neighbor sessions.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 6.x (2013), at 11-33.</p>	<p>A route reflector is configured to re-advertise routes learned through IGBP to a group of BGP neighbors within the AS (its clients), eliminating the need for a fully meshed topology. The <code>neighbor route-reflector-client</code> command configures the switch to act as a route reflector and configures the specified neighbor as one of its clients. The <code>bgp client-to-client reflection</code> command enables client-to-client reflection.</p> <p>When using route reflectors, an AS is divided into clusters. A cluster consists of one or more route reflectors and a group of clients to which they re-advertise route information. Multiple route reflectors can be configured in the same cluster to increase redundancy and avoid a single point of failure. Each route reflector has a cluster ID. If the cluster has a single route reflector, the cluster ID is its router ID. If a cluster has multiple route reflectors, a 4-byte cluster ID is assigned to all route reflectors in the cluster. All of them must be configured with the same cluster ID so that they can recognize updates from other route reflectors in the same cluster. The <code>bgp cluster-id</code> command configures the cluster ID in a cluster with multiple route reflectors.</p> <p>Example</p> <ul style="list-style-type: none"> These commands configure the switch as a route reflector and the neighbor at 101.72.14.5 as one of its clients, and set the cluster ID to 172.22.30.101. <pre>switch(config-router-bgp)#neighbor 101.72.14.5 route-reflector-client switch(config-router-bgp)#bgp cluster-id 172.22.30.101 switch(config-router-bgp)#</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1549.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1331; Arista User Manual, v. 4.11.1 (1/11/13), at 1081; Arista User Manual v. 4.10.3 (10/22/12), at 893; Arista User Manual v. 4.9.3.2 (5/3/12), at 665.</p>
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>Static routes have a default administrative distance of 1. A router prefers a static route to a dynamic route because the router considers a route with a low number to be the shortest. If you want a dynamic route to override a static route, you can specify an administrative distance for the static route. For example, if you have two dynamic routes with an administrative distance of 120, you would specify an administrative distance that is greater than 120 for the static route if you want the dynamic route to override the static route.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 6.x (2013), at 13-2.</p>	<p>Static routes have a default administrative distance of 1. Static routes with a higher administrative distance may be overridden by dynamic routing. For example, a static route with a distance of 200 is overridden by default OSPF intra-area routes (distance of 110). Route maps use tags to filter routes.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1720.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1153; Arista User Manual, v. 4.11.1 (1/11/13), at 914; Arista User Manual v. 4.10.3 (10/22/12), at 683.</p>

Copyright Registration Information	Cisco	Arista												
<div>Cisco NX-OS 6.2</div> <div>Effective date of registration: 11/13/2014</div>	<div><div>clear ip igmp interface statistics</div><div>To clear the IGMP statistics for an interface, use the <code>clear ip igmp interface statistics</code> command.</div><div><code>clear ip igmp interface statistics</code> <i>[if-type if-number]</i></div><table><tr><td>Syntax Description</td><td><i>if-type</i> (Optional) Interface type. For more information, use the question mark (?) online help function.</td></tr><tr><td></td><td><i>if-number</i> (Optional) Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.</td></tr></table><div>DefaultsNone</div><div>Command ModesAny command mode</div><div>SupportedUserRolesnetwork-admin network-operator vdc-admin vdc-operator</div><table><tr><td>Command History</td><td>ReleaseModification</td></tr><tr><td></td><td>4.0(3)This command was introduced.</td></tr></table><div>Usage GuidelinesThis command does not require a license.</div><div>ExamplesThis example shows how to clear IGMP statistics for an interface: <code>switch# clear ip igmp interface statistics ethernet 2/1</code> <code>switch#</code></div><div>Related Commands</div><table><tr><td>Command</td><td>Description</td></tr><tr><td><code>show ip igmp interface</code></td><td>Displays information about IGMP interfaces.</td></tr></table></div>	Syntax Description	<i>if-type</i> (Optional) Interface type. For more information, use the question mark (?) online help function.		<i>if-number</i> (Optional) Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.	Command History	ReleaseModification		4.0(3)This command was introduced.	Command	Description	<code>show ip igmp interface</code>	Displays information about IGMP interfaces.	<div><div>clear ip igmp statistics</div><div>The <code>clear ip igmp statistics</code> command resets IGMP transmission statistic counters for the specified interface.</div><div>Platformall Command ModePrivileged EXEC</div><div>Command Syntax</div><div><code>clear ip igmp statistics</code> <i>[INTF_ID]</i></div><div>Parameters</div><div><ul style="list-style-type: none"><i>INTF_ID</i> interface name. Options include:<ul style="list-style-type: none"><no parameter> all interfaces.interface ethernet <i>e_num</i> Ethernet interface specified by <i>e_num</i>.interface loopback <i>l_num</i> Loopback interface specified by <i>l_num</i>.interface management <i>m_num</i> Management interface specified by <i>m_num</i>.interface port-channel <i>p_num</i> Port-channel interface specified by <i>p_num</i>.interface vlan <i>v_num</i> VLAN interface specified by <i>v_num</i>.interface xlan <i>vx_num</i> VXLAN interface specified by <i>vx_num</i>.</div><div>Examples</div><div><ul style="list-style-type: none">This command resets IGMP transmission statistic counters on Ethernet 1 interface.<div><code>switch#clear ip igmp statistics interface ethernet 1</code> <code>switch#</code></div></div><div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1794.</div></div>
	Syntax Description	<i>if-type</i> (Optional) Interface type. For more information, use the question mark (?) online help function.												
	<i>if-number</i> (Optional) Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.													
Command History	ReleaseModification													
	4.0(3)This command was introduced.													
Command	Description													
<code>show ip igmp interface</code>	Displays information about IGMP interfaces.													

<div>Copyright Registration Information</div>	<div>Cisco</div>	<div>Arista</div>																				
<div>Cisco NX-OS 6.2</div> <div>Effective date of registration: 11/13/2014</div>	<div><div><div>ip igmp snooping last-member-query-interval</div><div>To configure a query interval in which the software removes a group, use the ip igmp snooping last-member-query-interval command. To reset the query interval to the default, use the no form of this command.</div><div><div>ip igmp snooping last-member-query-interval [interval]</div><div>no ip igmp snooping last-member-query-interval [interval]</div></div><table><tr><td>Syntax Description</td><td>interval Query interval in seconds. The range is from 1 to 25. The default is 1.</td></tr><tr><td>Defaults</td><td>The query interval is 1.</td></tr><tr><td>Command Modes</td><td>VLAN configuration (config-vlan) until Cisco NX-OS Release 5.1. Configure VLAN (config-vlan-config) since Cisco NX-OS Release 5.1(1). You cannot configure this command in the VLAN configuration mode in Cisco Release NX-OS 5.1 and higher.</td></tr><tr><td>Supported User Roles</td><td>network-admin vdc-admin</td></tr><tr><td>Command History</td><td><table><tr><th>Release</th><th>Modification</th></tr><tr><td>NX-OS 5.1(1)</td><td>The mode to configure this command on a VLAN changed to the configure VLAN mode (config-vlan-config)#. You can no longer configure this command in the VLAN configuration mode (config-vlan)#.</td></tr><tr><td>4.0(1)</td><td>This command was introduced.</td></tr></table></td></tr><tr><td>Usage Guidelines</td><td>This command does not require a license. See the Layer2 Command Reference Guide for information on entering the Configure VLAN mode by using the vlan configuration command.</td></tr><tr><td>Examples</td><td>This example shows how to configure a query interval in which the software removes a group: <pre>switch(config)# vlan configuration 10 switch(config-vlan-config)# ip igmp snooping last-member-query-interval 3 switch(config-vlan-config)#</pre> This example shows how to reset a query interval to the default: <pre>switch(config)# vlan configuration 10 switch(config-vlan-config)# no ip igmp snooping last-member-query-interval switch(config-vlan-config)#</pre></td></tr></table></div></div>	Syntax Description	interval Query interval in seconds. The range is from 1 to 25. The default is 1.	Defaults	The query interval is 1.	Command Modes	VLAN configuration (config-vlan) until Cisco NX-OS Release 5.1. Configure VLAN (config-vlan-config) since Cisco NX-OS Release 5.1(1). You cannot configure this command in the VLAN configuration mode in Cisco Release NX-OS 5.1 and higher.	Supported User Roles	network-admin vdc-admin	Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>NX-OS 5.1(1)</td><td>The mode to configure this command on a VLAN changed to the configure VLAN mode (config-vlan-config)#. You can no longer configure this command in the VLAN configuration mode (config-vlan)#.</td></tr><tr><td>4.0(1)</td><td>This command was introduced.</td></tr></table>	Release	Modification	NX-OS 5.1(1)	The mode to configure this command on a VLAN changed to the configure VLAN mode (config-vlan-config)#. You can no longer configure this command in the VLAN configuration mode (config-vlan)#.	4.0(1)	This command was introduced.	Usage Guidelines	This command does not require a license. See the Layer2 Command Reference Guide for information on entering the Configure VLAN mode by using the vlan configuration command.	Examples	This example shows how to configure a query interval in which the software removes a group: <pre>switch(config)# vlan configuration 10 switch(config-vlan-config)# ip igmp snooping last-member-query-interval 3 switch(config-vlan-config)#</pre> This example shows how to reset a query interval to the default: <pre>switch(config)# vlan configuration 10 switch(config-vlan-config)# no ip igmp snooping last-member-query-interval switch(config-vlan-config)#</pre>	<div><div><div>ip igmp last-member-query-interval</div><div>The ip igmp last-member-query-interval command configures the switch's transmission interval for sending group-specific or group-source-specific query messages from the configuration mode interface.</div><div>When a switch receives a message from a host that is leaving a group it sends query messages at intervals set by this command. The ip igmp startup-query-count specifies the number of messages that are sent before the switch stops forwarding packets to the host.</div><div>If the switch does not receive a response after this period, it stops forwarding traffic to the host on behalf of the group, source, or channel.</div><div>The no ip igmp last-member-query-interval and default ip igmp last-member-query-interval commands reset the query interval to the default value of one second by removing the ip igmp last-member-query-interval command from running-config.</div><div><div>Platformall</div><div>Command ModeInterface-Ethernet Configuration Interface-Port-Channel Configuration Interface-VLAN Configuration</div></div><div>Command Syntax<div><div>ip igmp last-member-query-interval period</div><div>no ip igmp last-member-query-interval</div><div>default ip igmp last-member-query-interval</div></div><div>Parameters<ul style="list-style-type: none">period transmission interval (deciseconds) between consecutive group-specific query messages. Value range: 10 (one second) to 317440 (8 hours, 49 minutes, 4 seconds). Default is 10 (one second).</div><div>Example<ul style="list-style-type: none">This command configures the last member query interval of 6 seconds for VLAN interface 4.<div><pre>switch(config)#interface vlan 4 switch(config-if-Vl4)#ip igmp last-member-query-interval 60 switch(config-if-Vl4)#</pre></div></div></div><div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1799.</div><div>See also Arista User Manual v. 4.12.3 (7/17/13), at 1519; Arista User Manual, v. 4.11.1 (1/11/13), at 1216; Arista User Manual v. 4.10.3 (10/22/12), at 1000; Arista User Manual v. 4.9.3.2 (5/3/12), at 785.</div></div></div>
	Syntax Description	interval Query interval in seconds. The range is from 1 to 25. The default is 1.																				
Defaults	The query interval is 1.																					
Command Modes	VLAN configuration (config-vlan) until Cisco NX-OS Release 5.1. Configure VLAN (config-vlan-config) since Cisco NX-OS Release 5.1(1). You cannot configure this command in the VLAN configuration mode in Cisco Release NX-OS 5.1 and higher.																					
Supported User Roles	network-admin vdc-admin																					
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>NX-OS 5.1(1)</td><td>The mode to configure this command on a VLAN changed to the configure VLAN mode (config-vlan-config)#. You can no longer configure this command in the VLAN configuration mode (config-vlan)#.</td></tr><tr><td>4.0(1)</td><td>This command was introduced.</td></tr></table>	Release	Modification	NX-OS 5.1(1)	The mode to configure this command on a VLAN changed to the configure VLAN mode (config-vlan-config)#. You can no longer configure this command in the VLAN configuration mode (config-vlan)#.	4.0(1)	This command was introduced.															
Release	Modification																					
NX-OS 5.1(1)	The mode to configure this command on a VLAN changed to the configure VLAN mode (config-vlan-config)#. You can no longer configure this command in the VLAN configuration mode (config-vlan)#.																					
4.0(1)	This command was introduced.																					
Usage Guidelines	This command does not require a license. See the Layer2 Command Reference Guide for information on entering the Configure VLAN mode by using the vlan configuration command.																					
Examples	This example shows how to configure a query interval in which the software removes a group: <pre>switch(config)# vlan configuration 10 switch(config-vlan-config)# ip igmp snooping last-member-query-interval 3 switch(config-vlan-config)#</pre> This example shows how to reset a query interval to the default: <pre>switch(config)# vlan configuration 10 switch(config-vlan-config)# no ip igmp snooping last-member-query-interval switch(config-vlan-config)#</pre>																					

Copyright Registration Information	Cisco	Arista																																																														
<div>Cisco NX-OS 6.2</div> <div>Effective date of registration: 11/13/2014</div>	<div><div>ip igmp snooping startup-query-count</div><div>To configure the number of queries sent at startup, use the <code>ip igmp snooping startup-query-count</code> command. To return to the default settings, use the <code>no</code> form of this command.</div><div><div>ip igmp snooping startup-query-count value</div><div>no ip igmp snooping startup-query-count value</div></div><table><tr><td>Syntax Description</td><td>value</td><td>Count value. The range is from 1 to 10.</td></tr><tr><td>Defaults</td><td colspan="2">None</td></tr><tr><td>Command Modes</td><td colspan="2">VLAN configuration (config-vlan)</td></tr><tr><td>Supported User Roles</td><td colspan="2">network-admin vdc-admin</td></tr><tr><td>Command History</td><td>Release</td><td>Modification</td></tr><tr><td></td><td>NX-OS 5.1(1)</td><td>This command was introduced.</td></tr><tr><td>Usage Guidelines</td><td colspan="2">This command does not require a license.</td></tr><tr><td>Examples</td><td colspan="2">This example shows how to configure the number of queries sent at startup: switch(config)# vlan configuration 10 switch(config-vlan-config)# ip igmp snooping startup-query-count 4 switch(config-vlan-config)#</td></tr><tr><td>Related Commands</td><td>Command</td><td>Description</td></tr><tr><td></td><td>show ip igmp snooping</td><td>Displays IGMP snooping information.</td></tr></table><div>Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference (2013), at 104.</div></div>	Syntax Description	value	Count value. The range is from 1 to 10.	Defaults	None		Command Modes	VLAN configuration (config-vlan)		Supported User Roles	network-admin vdc-admin		Command History	Release	Modification		NX-OS 5.1(1)	This command was introduced.	Usage Guidelines	This command does not require a license.		Examples	This example shows how to configure the number of queries sent at startup: switch(config)# vlan configuration 10 switch(config-vlan-config)# ip igmp snooping startup-query-count 4 switch(config-vlan-config)#		Related Commands	Command	Description		show ip igmp snooping	Displays IGMP snooping information.	<div><div>ip igmp snooping querier startup-query-count</div><div>The <code>ip igmp snooping querier startup-query-count</code> command configures the global <i>startup query count</i> value. The <i>startup query count</i> specifies the number of query messages that the querier sends on a VLAN during the <i>startup query interval</i> (<code>ip igmp snooping querier startup-query-interval</code>).</div><div>When snooping is enabled, the group state is more quickly established by sending query messages at a higher frequency. The <i>startup-query-interval</i> and <i>startup-query-count</i> parameters define the startup period by defining the number of queries to be sent and transmission frequency for these messages.</div><div>VLANs use the global <i>startup query count</i> value when they are not assigned a value (<code>ip igmp snooping vlan querier startup-query-count</code>). VLAN commands take precedence over the global value. The default global value is specified by the robustness variable (<code>ip igmp snooping robustness-variable</code>).</div><div>The <code>no ip igmp snooping querier startup-query-count</code> and default <code>ip igmp snooping querier startup-query-count</code> commands restore the default <i>startup-query-count</i> value by removing the corresponding <code>ip igmp snooping querier startup-query-count</code> command from <i>running-config</i>.</div><div><div>Platformall</div><div>Command ModeGlobal Configuration</div></div><div>Command Syntax<div><div>ip igmp snooping querier startup-query-count number</div><div>no ip igmp snooping querier startup-query-count</div><div>default ip igmp snooping querier startup-query-count</div></div><div>Parameters<ul style="list-style-type: none"><i>number</i> global startup query count. Value ranges from 1 to 3.</div><div>Example<ul style="list-style-type: none">These commands configure the global startup query count value of 2, then displays the status of the snooping querier.</div><div><div><div>switch(config)# ip igmp snooping querier startup-query-count 2</div><div>switch(config)# show ip igmp snooping querier status</div><div>Global IGMP Querier status</div><div>-----</div><div>admin state : Disabled</div><div>source IP address : 0.0.0.0</div><div>query-interval (sec) : 125.0</div><div>max-rsponse-time (sec) : 10.0</div><div>querier timeout (sec) : 255.0</div><div>last-member-query-interval (sec) : 1.0</div><div>last-member-query-count : 2 (robustness)</div><div>startup-query-interval (sec) : 31.25 (query-interval/4)</div><div>startup-query-count : 2</div><div>-----</div><div><table><tr><th>Vlan</th><th>Admin State</th><th>IP</th><th>Query Interval</th><th>Response Time</th><th>Querier Timeout</th><th>Operational State</th><th>Ver</th></tr><tr><td>1</td><td>Disabled</td><td>0.0.0.0</td><td>125.0</td><td>10.0</td><td>255.0</td><td>Non-Querier</td><td>v2</td></tr><tr><td>100</td><td>Disabled</td><td>0.0.0.0</td><td>125.0</td><td>10.0</td><td>255.0</td><td>Non-Querier</td><td>v2</td></tr><tr><td>101</td><td>Disabled</td><td>0.0.0.0</td><td>125.0</td><td>10.0</td><td>255.0</td><td>Non-Querier</td><td>v2</td></tr></table></div><div>switch(config)#</div></div></div></div><div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/201), at 1813.</div></div>	Vlan	Admin State	IP	Query Interval	Response Time	Querier Timeout	Operational State	Ver	1	Disabled	0.0.0.0	125.0	10.0	255.0	Non-Querier	v2	100	Disabled	0.0.0.0	125.0	10.0	255.0	Non-Querier	v2	101	Disabled	0.0.0.0	125.0	10.0	255.0	Non-Querier	v2
	Syntax Description	value	Count value. The range is from 1 to 10.																																																													
Defaults	None																																																															
Command Modes	VLAN configuration (config-vlan)																																																															
Supported User Roles	network-admin vdc-admin																																																															
Command History	Release	Modification																																																														
	NX-OS 5.1(1)	This command was introduced.																																																														
Usage Guidelines	This command does not require a license.																																																															
Examples	This example shows how to configure the number of queries sent at startup: switch(config)# vlan configuration 10 switch(config-vlan-config)# ip igmp snooping startup-query-count 4 switch(config-vlan-config)#																																																															
Related Commands	Command	Description																																																														
	show ip igmp snooping	Displays IGMP snooping information.																																																														
Vlan	Admin State	IP	Query Interval	Response Time	Querier Timeout	Operational State	Ver																																																									
1	Disabled	0.0.0.0	125.0	10.0	255.0	Non-Querier	v2																																																									
100	Disabled	0.0.0.0	125.0	10.0	255.0	Non-Querier	v2																																																									
101	Disabled	0.0.0.0	125.0	10.0	255.0	Non-Querier	v2																																																									

Copyright Registration Information	Cisco	Arista																																																								
<div>Cisco NX-OS 6.2</div> <div>Effective date of registration: 11/13/2014</div>	<div><div>ip igmp snooping startup-query-interval</div><div>To configure the query interval at startup, use the ip igmp snooping startup-query-interval command. To return to the default settings, use the no form of this command.</div><div><div>ip igmp snooping startup-query-interval sec</div><div>no ip igmp snooping startup-query-interval sec</div></div><table><tr><td>Syntax Description</td><td>secInterval in seconds. The range is from 1 to 18000.</td></tr><tr><td>Defaults</td><td>None</td></tr><tr><td>Command Modes</td><td>VLAN configuration (config-vlan)</td></tr><tr><td>Supported User Roles</td><td>network-admin vdc-admin</td></tr><tr><td>Command History</td><td><table><tr><th>Release</th><th>Modification</th></tr><tr><td>NX-OS 5.1(1)</td><td>This command was introduced.</td></tr></table></td></tr><tr><td>Usage Guidelines</td><td>This command does not require a license.</td></tr><tr><td>Examples</td><td><div>This example shows how to configure the query interval at startup:</div><div>switch(config)# vlan configuration 10 switch(config-vlan-config)# ip igmp snooping startup-query-interval 4 switch(config-vlan-config)#</div></td></tr><tr><td>Related Commands</td><td><table><tr><th>Command</th><th>Description</th></tr><tr><td>show ip igmp snooping</td><td>Displays IGMP snooping information.</td></tr></table></td></tr></table><div>Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference (2013), at 105.</div></div>	Syntax Description	secInterval in seconds. The range is from 1 to 18000.	Defaults	None	Command Modes	VLAN configuration (config-vlan)	Supported User Roles	network-admin vdc-admin	Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>NX-OS 5.1(1)</td><td>This command was introduced.</td></tr></table>	Release	Modification	NX-OS 5.1(1)	This command was introduced.	Usage Guidelines	This command does not require a license.	Examples	<div>This example shows how to configure the query interval at startup:</div> <div>switch(config)# vlan configuration 10 switch(config-vlan-config)# ip igmp snooping startup-query-interval 4 switch(config-vlan-config)#</div>	Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>show ip igmp snooping</td><td>Displays IGMP snooping information.</td></tr></table>	Command	Description	show ip igmp snooping	Displays IGMP snooping information.	<div><div>ip igmp snooping querier startup-query-interval</div><div>The ip igmp snooping querier startup-query-interval command configures the global startup query interval value. The startup query interval specifies the period between query messages that the querier sends upon startup.</div><div>When snooping is enabled, the group state is more quickly established by sending query messages at a higher frequency. The startup-query-interval and startup-query-count parameters define the startup period by defining the number of queries to be sent and transmission frequency for these messages.</div><div>VLANs use the global startup query interval value when they are not assigned a value (ip igmp snooping vlan querier startup-query-interval). VLAN commands take precedence over the global value. The default global value equals the query interval divided by four (ip igmp snooping querier query-interval).</div><div>The no ip igmp snooping querier startup-query-interval and default ip igmp snooping querier startup-query-interval commands restore the default method of specifying the startup query interval by removing the corresponding ip igmp snooping querier startup-query-interval command from running-config.</div><div><div>Platformall</div><div>Command ModeGlobal Configuration</div></div><div>Command Syntax<div><div>ip igmp snooping querier startup-query-interval period</div><div>no ip igmp snooping querier startup-query-interval</div><div>default ip igmp snooping querier startup-query-interval</div></div><div>Parameters<ul style="list-style-type: none">periodstartup query interval (seconds). Value ranges from 1 to 3600 (1 hour).</div><div>Example<ul style="list-style-type: none">This command configures the startup query count of one minute for VLAN interface 4.<div><div>switch(config)#ip igmp snooping querier startup-query-interval 40</div><div>switch(config)#show ip igmp snooping querier status</div><div>Global IGMP Querier status</div><div>-----</div><div>admin state: Enabled</div><div>source IP address: 0.0.0.0</div><div>query-interval (sec): 125.0</div><div>max-response-time (sec): 10.0</div><div>querier timeout (sec): 255.0</div><div>last-member-query-interval (sec): 1.0</div><div>last-member-query-count: 2 (robustness)</div><div>startup-query-interval (sec): 40.0</div><div>startup-query-count: 2</div><table><tr><th>Vlan</th><th>Admin State</th><th>IP</th><th>Query Interval</th><th>Response Time</th><th>Querier Timeout</th><th>Operational State</th><th>Ver</th></tr><tr><td>1</td><td>Enabled</td><td>0.0.0.0</td><td>125.0</td><td>10.0</td><td>255.0</td><td>Non-Querier</td><td>v3</td></tr><tr><td>100</td><td>Enabled</td><td>0.0.0.0</td><td>125.0</td><td>10.0</td><td>255.0</td><td>Non-Querier</td><td>v3</td></tr><tr><td>101</td><td>Enabled</td><td>0.0.0.0</td><td>125.0</td><td>10.0</td><td>255.0</td><td>Non-Querier</td><td>v3</td></tr></table><div>switch(config)#</div></div></div><div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1813.</div></div></div>	Vlan	Admin State	IP	Query Interval	Response Time	Querier Timeout	Operational State	Ver	1	Enabled	0.0.0.0	125.0	10.0	255.0	Non-Querier	v3	100	Enabled	0.0.0.0	125.0	10.0	255.0	Non-Querier	v3	101	Enabled	0.0.0.0	125.0	10.0	255.0	Non-Querier	v3
	Syntax Description	secInterval in seconds. The range is from 1 to 18000.																																																								
Defaults	None																																																									
Command Modes	VLAN configuration (config-vlan)																																																									
Supported User Roles	network-admin vdc-admin																																																									
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>NX-OS 5.1(1)</td><td>This command was introduced.</td></tr></table>	Release	Modification	NX-OS 5.1(1)	This command was introduced.																																																					
Release	Modification																																																									
NX-OS 5.1(1)	This command was introduced.																																																									
Usage Guidelines	This command does not require a license.																																																									
Examples	<div>This example shows how to configure the query interval at startup:</div> <div>switch(config)# vlan configuration 10 switch(config-vlan-config)# ip igmp snooping startup-query-interval 4 switch(config-vlan-config)#</div>																																																									
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>show ip igmp snooping</td><td>Displays IGMP snooping information.</td></tr></table>	Command	Description	show ip igmp snooping	Displays IGMP snooping information.																																																					
Command	Description																																																									
show ip igmp snooping	Displays IGMP snooping information.																																																									
Vlan	Admin State	IP	Query Interval	Response Time	Querier Timeout	Operational State	Ver																																																			
1	Enabled	0.0.0.0	125.0	10.0	255.0	Non-Querier	v3																																																			
100	Enabled	0.0.0.0	125.0	10.0	255.0	Non-Querier	v3																																																			
101	Enabled	0.0.0.0	125.0	10.0	255.0	Non-Querier	v3																																																			

Copyright Registration Information	Cisco	Arista																														
<div>Cisco NX-OS 6.2</div> <div>Effective date of registration: 11/13/2014</div>	<div><div>ip igmp snooping version</div><div>To configure the IGMP version number for VLAN, use the <code>ip igmp snooping version</code> command. To return to the default settings, use the no form of this command.</div><div><div>ip igmp snooping version value</div><div>no ip igmp snooping version value</div></div><table><tr><td>Syntax Description</td><td>value</td><td>Version number value. The range is from 2 to 3.</td></tr><tr><td>Defaults</td><td colspan="2">None</td></tr><tr><td>Command Modes</td><td colspan="2">VLAN configuration (config-vlan)</td></tr><tr><td>Supported User Roles</td><td colspan="2">network-admin vde-admin</td></tr><tr><td>Command History</td><td>Release</td><td>Modification</td></tr><tr><td></td><td>5.1(1)</td><td>This command was introduced.</td></tr><tr><td>Usage Guidelines</td><td colspan="2">This command does not require a license.</td></tr><tr><td>Examples</td><td colspan="2">This example shows how to configure IGMP version number for VLAN: <div>switch(config-vlan-config)# ip igmp snooping version 3</div><div>switch(config-vlan-config)#</div></td></tr><tr><td>Related Commands</td><td>Command</td><td>Description</td></tr><tr><td></td><td>show ip igmp snooping</td><td>Displays IGMP snooping information.</td></tr></table><div>Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference (2013), at 108.</div></div>	Syntax Description	value	Version number value. The range is from 2 to 3.	Defaults	None		Command Modes	VLAN configuration (config-vlan)		Supported User Roles	network-admin vde-admin		Command History	Release	Modification		5.1(1)	This command was introduced.	Usage Guidelines	This command does not require a license.		Examples	This example shows how to configure IGMP version number for VLAN: <div>switch(config-vlan-config)# ip igmp snooping version 3</div> <div>switch(config-vlan-config)#</div>		Related Commands	Command	Description		show ip igmp snooping	Displays IGMP snooping information.	<div><div>ip igmp snooping querier version</div><div>The <code>ip igmp snooping querier version</code> command configures the Internet Group Management Protocol (IGMP) snooping querier version on the configuration mode interfaces. Version 3 is the default IGMP version.</div><div>IGMP is enabled by the <code>ip pim sparse-mode</code> command. The <code>ip igmp snooping querier version</code> command does not affect the IGMP enabled status.</div><div>The <code>no ip igmp snooping querier version</code> and default <code>ip igmp snooping querier version</code> commands restore the configuration mode to IGMP version 3 by removing the <code>ip igmp snooping querier version</code> statement from <i>running-config</i>.</div><div><div>Platform</div><div>all</div><div>Command Mode</div><div>Global Configuration</div></div><div>Command Syntax</div><div><div>ip igmp snooping querier version version_number</div><div>no ip igmp snooping querier version</div><div>default ip igmp snooping querier version</div></div><div>Parameters</div><div><div>version_number</div><div>IGMP version number. Value ranges from 1 to 3. Default value is 3.</div></div><div>Example</div><div><div>This command configures IGMP snooping querier version 2.</div><div><div>switch(config)# ip igmp snooping querier version 2</div><div>switch(config)#</div></div><div>This command restores the IGMP snooping querier to version 2.</div><div><div>switch(config)# no ip igmp snooping querier version</div><div>switch(config)#</div></div></div><div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1815.</div><div>See also Arista User Manual v. 4.12.3 (7/17/13), at 1531.</div></div>
	Syntax Description	value	Version number value. The range is from 2 to 3.																													
Defaults	None																															
Command Modes	VLAN configuration (config-vlan)																															
Supported User Roles	network-admin vde-admin																															
Command History	Release	Modification																														
	5.1(1)	This command was introduced.																														
Usage Guidelines	This command does not require a license.																															
Examples	This example shows how to configure IGMP version number for VLAN: <div>switch(config-vlan-config)# ip igmp snooping version 3</div> <div>switch(config-vlan-config)#</div>																															
Related Commands	Command	Description																														
	show ip igmp snooping	Displays IGMP snooping information.																														

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>Examples</p> <p>This example shows how to display information about IGMP snooping queriers:</p> <pre>switch(config)# show ip igmp snooping querier Vlan IP Address Version Port 1 172.20.50.11 v3 fa2/1 2 172.20.40.20 v2 Router switch(config)#</pre> <p>Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference (2013), at 50.</p>	<p>Example</p> <ul style="list-style-type: none"> This command displays the querier IP address, version, and port servicing each VLAN. <pre>switch>show ip igmp snooping querier Vlan IP Address Version Port ----- 1 172.17.0.37 v2 Po1 20 172.17.20.1 v2 Po1 26 172.17.26.1 v2 Cpu 2028 172.17.255.29 v2 Po1 switch></pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1860.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1568; Arista User Manual, v. 4.11.1 (1/11/13), at 1263; Arista User Manual v. 4.10.3 (10/22/12), at 1074; Arista User Manual v. 4.9.3.2 (5/3/12), at 831; Arista User Manual v. 4.8.2 (11/18/11), at 637.</p>

Copyright Registration Information	Cisco	Arista																												
<div>Cisco NX-OS 6.2</div> <div>Effective date of registration: 11/13/2014</div>	<div><div>aaa group server tacacs+</div><div>To create a TACACS+ server group and enter TACACS+ server group configuration mode, use the <code>aaa group server tacacs+</code> command. To delete a TACACS+ server group, use the <code>no</code> form of this command.</div><div><div>aaa group server tacacs+ group-name</div><div>no aaa group server tacacs+ group-name</div></div><div><table><tr><td>Syntax Description</td><td>group-name</td><td>TACACS+ server group name. The name is alphanumeric and case-sensitive. The maximum length is 64 characters.</td></tr><tr><td>Defaults</td><td colspan="2">None</td></tr><tr><td>Command Modes</td><td colspan="2">Global configuration</td></tr><tr><td>Supported User Roles</td><td colspan="2">network-admin vdc-admin</td></tr><tr><td>Command History</td><td>Release</td><td>Modification</td></tr><tr><td></td><td>4.0(1)</td><td>This command was introduced.</td></tr><tr><td>Usage Guidelines</td><td colspan="2">You must use the <code>feature tacacs+</code> command before you configure TACACS+. This command does not require a license.</td></tr><tr><td>Examples</td><td colspan="2"><div>This example shows how to create a TACACS+ server group and enter TACACS+ server configuration mode:</div><div>switch# configure terminal switch(config)# aaa group server tacacs+ TacServer switch(config-radius)#</div><div>This example shows how to delete a TACACS+ server group:</div><div>switch# configure terminal switch(config)# no aaa group server tacacs+ Tacserver</div></td></tr></table></div></div>	Syntax Description	group-name	TACACS+ server group name. The name is alphanumeric and case-sensitive. The maximum length is 64 characters.	Defaults	None		Command Modes	Global configuration		Supported User Roles	network-admin vdc-admin		Command History	Release	Modification		4.0(1)	This command was introduced.	Usage Guidelines	You must use the <code>feature tacacs+</code> command before you configure TACACS+. This command does not require a license.		Examples	<div>This example shows how to create a TACACS+ server group and enter TACACS+ server configuration mode:</div> <div>switch# configure terminal switch(config)# aaa group server tacacs+ TacServer switch(config-radius)#</div> <div>This example shows how to delete a TACACS+ server group:</div> <div>switch# configure terminal switch(config)# no aaa group server tacacs+ Tacserver</div>		<div><div>aaa group server tacacs+</div><div>The <code>aaa group server tacacs+</code> command enters <code>server-group-tacacs+</code> configuration mode for the specified group name. The command creates the specified group if it was not previously created. Commands are available to add servers to the group.</div><div>A server group is a collection of servers that are associated with a single label. Subsequent authorization and authentication commands access all servers in a group by invoking the group name. Server group members must be previously configured with a <code>tacacs-server host</code> command.</div><div>The <code>no aaa group server tacacs+</code> and default <code>aaa group server tacacs+</code> commands delete the specified server group from <i>running-config</i>.</div><div><table><tr><td>Platform</td><td>all</td></tr><tr><td>Command Mode</td><td>Global Configuration</td></tr></table></div><div>Command Syntax<div><div>aaa group server tacacs+ group name</div><div>no aaa group server tacacs+ group_name</div><div>default aaa group server tacacs+ group_name</div></div></div><div>Parameters<ul style="list-style-type: none"><code>group_name</code> name (text string) assigned to the group. Cannot be identical to a name already assigned to a RADIUS server group.</div><div>Commands Available in <code>server-group-tacacs+</code> Configuration Mode<ul style="list-style-type: none"><code>server</code> (<code>server-group-TACACS+ configuration mode</code>)</div><div>Related Commands<ul style="list-style-type: none"><code>aaa group server radius</code></div><div>Example<ul style="list-style-type: none">This command creates the TACACS+ server group named TAC-GR and enters server group configuration mode for the new group.<div><div>switch(config)#aaa group server tacacs+ TAC-GR</div><div>switch(ccnfig-sg-tacacs+TAC-GR)#</div></div></div><div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 225.</div><div>See also Arista User Manual v. 4.12.3 (7/17/13), at 169; Arista User Manual, v. 4.11.1 (1/11/13), at 127; Arista User Manual v. 4.10.3 (10/22/12), at 119.</div></div>	Platform	all	Command Mode	Global Configuration
	Syntax Description	group-name	TACACS+ server group name. The name is alphanumeric and case-sensitive. The maximum length is 64 characters.																											
Defaults	None																													
Command Modes	Global configuration																													
Supported User Roles	network-admin vdc-admin																													
Command History	Release	Modification																												
	4.0(1)	This command was introduced.																												
Usage Guidelines	You must use the <code>feature tacacs+</code> command before you configure TACACS+. This command does not require a license.																													
Examples	<div>This example shows how to create a TACACS+ server group and enter TACACS+ server configuration mode:</div> <div>switch# configure terminal switch(config)# aaa group server tacacs+ TacServer switch(config-radius)#</div> <div>This example shows how to delete a TACACS+ server group:</div> <div>switch# configure terminal switch(config)# no aaa group server tacacs+ Tacserver</div>																													
Platform	all																													
Command Mode	Global Configuration																													

Copyright Registration Information	Cisco	Arista					
<div>Cisco NX-OS 6.2</div> <div>Effective date of registration: 11/13/2014</div>	<div><div>dot1x pae authenticator</div><div>To create the 802.1X authenticator port access entity (PAE) role for an interface, use the dot1x pae authenticator command. To remove the 802.1X authenticator PAE role, use the no form of this command.</div><div><div>dot1x pae authenticator</div><div>no dot1x pae authenticator</div></div><div><div>Syntax Description</div><div>This command has no arguments or keywords.</div></div><div><div>Defaults</div><div>802.1X automatically creates the authenticator PAE when you enable the feature on an interface.</div></div><div><div>Command Modes</div><div>Interface configuration</div></div><div><div>Supported User Roles</div><div>network-admin vdc-admin</div></div><div><div>Command History</div><table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.2(1)</td><td>This command was introduced.</td></tr></table></div><div><div>Usage Guidelines</div><div><div>You must use the feature dot1x command before you configure 802.1X.</div><div>When you enable 802.1X on an interface, the Cisco NX-OS software creates an authenticator port access entity (PAE) instance. An authenticator PAE is a protocol entity that supports authentication on the interface. When you disable 802.1X on the interface, the Cisco NX-OS software does not automatically clear the authenticator PAE instances. You can explicitly remove the authenticator PAE from the interface and then reapply it, as needed.</div><div>This command does not require a license.</div></div></div><div><div>Examples</div><div><div>This example shows how to create the 802.1X authenticator PAE role on an interface:</div><div>switch# configure terminal switch(config)# interface ethernet 2/4 switch(config-if)# dot1x pae authenticator</div><div>This example shows how to remove the 802.1X authenticator PAE role from an interface:</div><div>switch# configure terminal switch(config)# interface ethernet 2/4 switch(config-if)# no dot1x pae authenticator</div></div></div></div>	Release	Modification	4.2(1)	This command was introduced.	<div><div>dot1x pae authenticator</div><div>The dot1x pae authenticator command sets the Port Access Entity (PAE) type. The interface acts only as an authenticator and will not respond to any messages meant for a supplicant.</div><div>The no dot1x pae authenticator and default dot1x pae authenticator commands restore the switch default by deleting the corresponding dot1x pae authenticator command from <i>running-config</i>.</div><div><div>Platform</div><div>all</div></div><div><div>Command Mode</div><div>Interface-Ethernet Configuration Interface-Management Configuration</div></div><div><div>Command Syntax</div><div><div>dot1x pae authenticator</div><div>no dot1x pae authenticator</div><div>default dot1x pae authenticator</div></div></div><div><div>Example</div><div><div><ul style="list-style-type: none">This command configures the port as an IEEE 802.1x port access entity (PAE) authenticator, which enables IEEE 802.1x on the port but does not allow clients connected to the port to be authorized, use the dot1x pae authenticator interface configuration command.</div><div><div>switch(config-if-Et1)#interface ethernet 2</div><div>switch(config-if-Et1)#dot1x pae authenticator</div><div>switch(config-if-Et1)#</div></div><div><div><ul style="list-style-type: none">This example shows how to disable IEEE 802.1x authentication on the port.</div><div><div>switch(config-if-Et1)#interface ethernet 2</div><div>switch(config-if-Et1)#no dot1x pae authenticator</div><div>switch(config-if-Et1)#</div></div></div></div></div></div>	<div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 566.</div>
	Release	Modification					
4.2(1)	This command was introduced.						

Copyright Registration Information	Cisco	Arista
<div>Cisco NX-OS 6.2</div> <div>Effective date of registration: 11/13/2014</div>	<div><div>dot1x timeout quiet-period</div><div>To configure the 802.1X quiet-period timeout globally or for an interface, use the <code>dot1x timeout quiet-period</code> command. To revert to the default, use the <code>no</code> form of this command.</div><div><div>dot1x timeout quiet-period seconds</div><div>no dot1x timeout quiet-period</div></div><div><div><div>Syntax Description</div><div>seconds</div><div>Number of seconds for the 802.1X quiet-period timeout. The range is from 1 to 65535.</div></div><div><div>Defaults</div><div>Global configuration: 60 seconds Interface configuration: The value of the global configuration</div></div><div><div>Command Modes</div><div>Global configuration Interface configuration</div></div><div><div>Supported User Roles</div><div>network-admin vdc-admin</div></div><div><div><div>Command History</div><div><div>Release</div><div>Modification</div></div><div><div>4.0(1)</div><div>This command was introduced.</div></div></div><div><div><div>Usage Guidelines</div><div>The 802.1X quiet-period timeout is the number of seconds that the device remains in the quiet state following a failed authentication exchange with a supplicant. You must use the <code>feature dot1x</code> command before you configure 802.1X.</div></div><div><div><div>Note</div><div>You should change the default value only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain supplicants and authentication servers.</div></div><div>This command does not require a license.</div></div><div><div><div>Examples</div><div>This example shows how to configure the global 802.1X quiet-period timeout: switch# configure terminal switch(config)# dot1x timeout quiet-period 45</div></div></div></div><div>Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-200.</div></div></div></div>	<div><div>dot1x timeout quiet-period</div><div>The <code>dot1x timeout quiet-period</code> command sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client. The range is 1 to 65535 seconds; the default is 60.</div><div>When the switch cannot authenticate the client, the switch remains idle for a set period of time and then tries again. You can provide a faster response time to the user by entering a number smaller than the default.</div><div>The <code>no dot1x timeout quiet-period</code> and default <code>dot1x timeout quiet-period</code> commands restore the default advertisement interval of 60 seconds by removing the corresponding <code>dot1x timeout quiet-period</code> command from <i>running-config</i>.</div><div><div><div>Platform</div><div>all</div></div><div><div>Command Mode</div><div>Interface-Ethernet Configuration Interface-Management Configuration</div></div></div><div><div>Command Syntax</div><div><div>dot1x timeout quiet-period quiet_time</div><div>no dot1x timeout quiet-period</div><div>default dot1x timeout quiet-period</div></div><div><div>Parameters</div><div><div>quiet_time</div><div>advertisement interval (seconds). Values range from 1 to 65535. Default value is 60.</div></div></div><div><div>Example</div><div><div><div>This command sets the number of seconds that an authenticator port waits after a failed authentication with a client before accepting authentication requests again.</div><div><div>switch(config)#interface Ethernet 1</div><div>switch(config-if-Et1)#dot1x timeout quiet-period 600</div><div>switch(config-if-Et1)#</div></div></div></div><div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 569.</div></div></div></div>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>To use this command, you must enable the DHCP snooping feature (see the <code>feature dhcp</code> command). You can configure up to four DHCP server IP addresses on Layer 3 Ethernet interfaces and subinterfaces, VLAN interfaces, and Layer 3 port channels. In Cisco NX-OS Release 4.0.2 and earlier releases, you can configure only one DHCP server IP address on an interface.</p> <p>When an inbound DHCP BOOTREQUEST packet arrives on the interface, <u>the relay agent forwards the packet to all DHCP server IP addresses specified on that interface. The relay agent forwards replies from all DHCP servers to the host that sent the request.</u></p> <p>This command does not require a license.</p> <p>Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-309.</p>	<p>The <code>ip dhcp snooping information option</code> command enables the insertion of option-82 DHCP snooping information in DHCP packets on VLANs where DHCP snooping is enabled. DHCP snooping is a layer 2 switch process that allows relay agents to provide remote-ID and circuit-ID information to DHCP reply and request packets. DHCP servers use this information to determine the originating port of DHCP requests and associate a corresponding IP address to that port.</p> <p>DHCP snooping uses information option (Option-82) to include the switch MAC address (router-ID) along with the physical interface name and VLAN number (circuit-ID) in DHCP packets. After adding the information to the packet, <u>the DHCP relay agent forwards the packet to the DHCP server</u> through DHCP protocol processes.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1270.</p>

Copyright Registration Information	Cisco	Arista														
<div>Cisco NX-OS 6.2</div> <div>Effective date of registration: 11/13/2014</div>	<div><div>ip dhcp relay information option</div><div>To enable the device to insert and remove option-82 information on DHCP packets forwarded by the relay agent, use the <code>ip dhcp relay information option</code> command. To disable the insertion and removal of option-82 information, use the <code>no ip dhcp relay information option</code> command.</div><div><div>ip dhcp relay information option</div><div>no ip dhcp relay information option</div></div><div><div>Syntax Description</div><div>This command has no arguments or keywords.</div></div><div><div>Defaults</div><div>By default, the device does not insert and remove option-82 information on DHCP packets forwarded by the relay agent.</div></div><div><div>Command Modes</div><div>Global configuration</div></div><div><div>Supported User Roles</div><div>network-admin vdc-admin</div></div><div><div>Command History</div><table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.0(1)</td><td>This command was introduced.</td></tr></table></div><div><div>Usage Guidelines</div><div>To use this command, you must enable the DHCP snooping feature (see the <code>feature dhcp</code> command). This command does not require a license.</div></div><div><div>Examples</div><div>This example shows how to enable the DHCP relay agent to insert and remove option-82 information to and from packets it forwards: <pre>switch# configure terminal switch(config)# ip dhcp relay information option switch(config)#</pre></div></div><div><div>Related Commands</div><table><tr><th>Command</th><th>Description</th></tr><tr><td>ip dhcp relay</td><td>Enables or disables the DHCP relay agent.</td></tr><tr><td>ip dhcp relay address</td><td>Configures the IP address of a DHCP server on an interface.</td></tr><tr><td>ip dhcp relay sub-option type cisco</td><td>Enables DHCP to use Cisco proprietary numbers 150, 152, and 151 when filling the link selection, server ID override, and VRF name/VPN ID relay agent option-82 suboptions.</td></tr><tr><td>ip dhcp snooping</td><td>Globally enables DHCP snooping on the device.</td></tr></table></div></div>	Release	Modification	4.0(1)	This command was introduced.	Command	Description	ip dhcp relay	Enables or disables the DHCP relay agent.	ip dhcp relay address	Configures the IP address of a DHCP server on an interface.	ip dhcp relay sub-option type cisco	Enables DHCP to use Cisco proprietary numbers 150, 152, and 151 when filling the link selection, server ID override, and VRF name/VPN ID relay agent option-82 suboptions.	ip dhcp snooping	Globally enables DHCP snooping on the device.	<div><div>ip dhcp relay information option (Global)</div><div>The <code>ip dhcp relay information option</code> command configures the switch to attach tags to DHCP requests before forwarding them to the DHCP servers designated by <code>ip helper-address</code> commands. The <code>ip dhcp relay information option circuit-id</code> command specifies the tag contents for packets forwarded by the interface that it configures.</div><div>The <code>no ip dhcp relay information option</code> and default <code>ip dhcp relay information option</code> commands restore the switch's default setting of not attaching tags to DHCP requests by removing the <code>ip dhcp relay information option</code> command from <i>running-config</i>.</div><div><div>Platform</div><div>all</div></div><div><div>Command Mode</div><div>Global Configuration</div></div><div><div>Command Syntax</div><div><div>ip dhcp relay information option</div><div>no ip dhcp relay information option</div><div>default ip dhcp relay information option</div></div></div><div><div>Related Commands</div><div>These commands implement DHCP relay agent.</div><div><ul style="list-style-type: none">ip helper-addressip dhcp relay always-onip dhcp relay information option circuit-id</div></div><div><div>Example</div><div><ul style="list-style-type: none">This command enables the attachment of tags to DHCP requests that are forwarded to DHCP server addresses.<div><pre>switch(config)#ip dhcp relay information option switch(config)#</pre></div></div></div><div><div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1264.</div><div>See also Arista User Manual v. 4.12.3 (7/17/13), at 1068; Arista User Manual, v. 4.11.1 (1/11/13), at 852; Arista User Manual v. 4.10.3 (10/22/12), at 701.</div></div></div>
	Release	Modification														
4.0(1)	This command was introduced.															
Command	Description															
ip dhcp relay	Enables or disables the DHCP relay agent.															
ip dhcp relay address	Configures the IP address of a DHCP server on an interface.															
ip dhcp relay sub-option type cisco	Enables DHCP to use Cisco proprietary numbers 150, 152, and 151 when filling the link selection, server ID override, and VRF name/VPN ID relay agent option-82 suboptions.															
ip dhcp snooping	Globally enables DHCP snooping on the device.															

Copyright Registration Information	Cisco	Arista															
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<table><tr><th>Related Commands</th><th>Command</th><th>Description</th></tr><tr><td></td><td>ip dhcp relay</td><td>Enables or disables the DHCP relay agent.</td></tr><tr><td></td><td>ip dhcp relay address</td><td>Configures the IP address of a DHCP server on an interface.</td></tr><tr><td></td><td>ip dhcp relay sub-option type cisco</td><td>Enables DHCP to use Cisco proprietary numbers 150, 152, and 151 when filling the link selection, server ID override, and VRF name/VPN ID relay agent option-82 suboptions.</td></tr><tr><td></td><td>ip dhcp snooping</td><td>Globally enables DHCP snooping on the device.</td></tr></table> Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-311.	Related Commands	Command	Description		ip dhcp relay	Enables or disables the DHCP relay agent.		ip dhcp relay address	Configures the IP address of a DHCP server on an interface.		ip dhcp relay sub-option type cisco	Enables DHCP to use Cisco proprietary numbers 150, 152, and 151 when filling the link selection, server ID override, and VRF name/VPN ID relay agent option-82 suboptions.		ip dhcp snooping	Globally enables DHCP snooping on the device.	<p>Related Commands</p> <ul style="list-style-type: none">• ip dhcp snooping globally enables DHCP snooping.• ip dhcp snooping vlan enables DHCP snooping on specified VLANs.• ip helper-address enables the DHCP relay agent on a configuration mode interface. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1270.
Related Commands	Command	Description															
	ip dhcp relay	Enables or disables the DHCP relay agent.															
	ip dhcp relay address	Configures the IP address of a DHCP server on an interface.															
	ip dhcp relay sub-option type cisco	Enables DHCP to use Cisco proprietary numbers 150, 152, and 151 when filling the link selection, server ID override, and VRF name/VPN ID relay agent option-82 suboptions.															
	ip dhcp snooping	Globally enables DHCP snooping on the device.															
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<p>Examples</p> <p>This example shows how to enable VRF support for the DHCP relay agent, which is dependent upon enabling Option-82 support for the DHCP relay agent, and how to configure a DHCP server address on a Layer 3 interface when the DHCP server is in a VRF named SiteA:</p> <pre>switch# configure terminal switch(config)# ip dhcp relay information option switch(config)# ip dhcp relay information option vpn switch(config)# interface ethernet 1/3 switch(config-if)# ip dhcp relay address 10.43.87.132 use-vrf SiteA switch(config-if)#</pre> Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-314.	<p>Example</p> <ul style="list-style-type: none">• This command enables the attachment of tags to DHCP requests that are forwarded to DHCP server addresses. <pre>switch(config)#ip dhcp relay information option switch(config)#</pre> Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1237. See also Arista User Manual v. 4.12.3 (7/17/13), at 1068; Arista User Manual, v. 4.11.1 (1/11/13), at 852; Arista User Manual v. 4.10.3 (10/22/12), at 688.															
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<table><tr><th>Command</th><th>Description</th></tr><tr><td>feature dhcp</td><td>Enables the DHCP snooping feature on the device.</td></tr><tr><td>ip dhcp relay</td><td>Enables the DHCP relay agent.</td></tr><tr><td>ip dhcp relay address</td><td>Configures an IP address of a DHCP server on an interface.</td></tr><tr><td>ip dhcp relay information option</td><td>Enables the insertion and removal of option-82 information from DHCP packets forwarded by the DHCP relay agent.</td></tr><tr><td>ip dhcp snooping</td><td>Globally enables DHCP snooping on the device.</td></tr></table> Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-317.	Command	Description	feature dhcp	Enables the DHCP snooping feature on the device.	ip dhcp relay	Enables the DHCP relay agent.	ip dhcp relay address	Configures an IP address of a DHCP server on an interface.	ip dhcp relay information option	Enables the insertion and removal of option-82 information from DHCP packets forwarded by the DHCP relay agent.	ip dhcp snooping	Globally enables DHCP snooping on the device.	<p>Example</p> <ul style="list-style-type: none">• This command enables the DHCP relay agent. <pre>switch(config)#ip dhcp relay always-on switch(config)#</pre> Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1263. See also Arista User Manual v. 4.12.3 (7/17/13), at 1047; Arista User Manual, v. 4.11.1 (1/11/13), at 890; Arista User Manual v. 4.10.3 (10/22/12), at 688.			
Command	Description																
feature dhcp	Enables the DHCP snooping feature on the device.																
ip dhcp relay	Enables the DHCP relay agent.																
ip dhcp relay address	Configures an IP address of a DHCP server on an interface.																
ip dhcp relay information option	Enables the insertion and removal of option-82 information from DHCP packets forwarded by the DHCP relay agent.																
ip dhcp snooping	Globally enables DHCP snooping on the device.																

Copyright Registration Information	Cisco	Arista						
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<div>ip dhcp smart-relay</div> <p>To enable Dynamic Host Configuration Protocol (DHCP) smart relay on a Layer 3 interface, use the <code>ip dhcp smart-relay</code> command. To disable DHCP smart relay on a Layer 3 interface, use the <code>no</code> form of this command.</p> <div>ip dhcp smart-relay</div> <div>no ip dhcp smart-relay</div> <div><div>Syntax Description</div><div>This command has no arguments or keywords.</div></div> <div><div>Defaults</div><div>Disabled</div></div> <div><div>Command Modes</div><div>Interface configuration mode (config-if)</div></div> <div><div>Supported User Roles</div><div>network-admin vdc-admin</div></div> <p>Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-319.</p>	<div>ip dhcp smart-relay</div> <p>The <code>ip dhcp smart-relay</code> command configures the DHCP smart relay status on the configuration mode interface. DHCP smart relay supports forwarding DHCP requests with a client's secondary IP addresses in the gateway address field. Enabling DHCP smart relay on an interface requires that DHCP relay is also enabled on that interface.</p> <p>By default, an interface assumes the global DHCP smart relay setting as configured by the <code>ip dhcp smart-relay global</code> command. The <code>ip dhcp smart-relay</code> command, when configured, takes precedence over the global smart relay setting.</p> <p>The <code>no ip dhcp smart-relay</code> command disables DHCP smart relay on the configuration mode interface. The default <code>ip dhcp smart-relay</code> command restores the interface's to the default DHCP smart relay setting, as configured by the <code>ip dhcp smart-relay global</code> command, by removing the corresponding <code>ip dhcp smart-relay</code> or <code>no ip dhcp smart-relay</code> statement from <i>running-config</i>.</p> <div><div>Platform</div><div>all</div></div> <div><div>Command Mode</div><div>Interface-Ethernet Configuration Interface-Port-channel Configuration Interface-VLAN Configuration</div></div> <div><div>Command Syntax</div><div>ip dhcp smart-relay no ip dhcp smart-relay default ip dhcp smart-relay</div></div> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1266.</p>						
	Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<div><div>Related Commands</div><table><thead><tr><th>Command</th><th>Description</th></tr></thead><tbody><tr><td>ip dhcp smart-relay</td><td>Enables DHCP smart relay on a Layer 3 interface.</td></tr><tr><td>ip dhcp relay</td><td>Enable the DHCP relay agent.</td></tr></tbody></table></div> <p>Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-322.</p>	Command	Description	ip dhcp smart-relay	Enables DHCP smart relay on a Layer 3 interface.	ip dhcp relay	Enable the DHCP relay agent.
Command	Description							
ip dhcp smart-relay	Enables DHCP smart relay on a Layer 3 interface.							
ip dhcp relay	Enable the DHCP relay agent.							

Copyright Registration Information	Cisco	Arista												
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<div>Examples</div> <div>This example shows how to globally enable DHCP snooping:</div> <pre>switch# configure terminal switch(config)# ip dhcp snooping switch(config)#</pre> <div>Related Commands</div> <table><thead><tr><th>Command</th><th>Description</th></tr></thead><tbody><tr><td>feature dhcp</td><td>Enables the DHCP snooping feature on the device.</td></tr><tr><td>ip dhcp relay</td><td>Enables or disables the DHCP relay agent.</td></tr><tr><td>ip dhcp snooping information option</td><td>Enables the insertion and removal of option-82 information for DHCP packets forwarded without the use of the DHCP relay agent.</td></tr><tr><td>ip dhcp snooping trust</td><td>Configures an interface as a trusted source of DHCP messages.</td></tr><tr><td>ip dhcp snooping vlan</td><td>Enables DHCP snooping on the specified VLANs.</td></tr></tbody></table> <div>Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-323.</div>	Command	Description	feature dhcp	Enables the DHCP snooping feature on the device.	ip dhcp relay	Enables or disables the DHCP relay agent.	ip dhcp snooping information option	Enables the insertion and removal of option-82 information for DHCP packets forwarded without the use of the DHCP relay agent.	ip dhcp snooping trust	Configures an interface as a trusted source of DHCP messages.	ip dhcp snooping vlan	Enables DHCP snooping on the specified VLANs.	<div>Command Syntax</div> <pre>ip dhcp snooping no ip dhcp snooping default ip dhcp snooping</pre> <div>Related Commands</div> <ul style="list-style-type: none">• ip dhcp snooping information option enables insertion of option-82 snooping data.• ip dhcp snooping vlan enables DHCP snooping on specified VLANs.• ip helper-address enables the DHCP relay agent on a configuration mode interface. <div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1269.</div>
	Command	Description												
feature dhcp	Enables the DHCP snooping feature on the device.													
ip dhcp relay	Enables or disables the DHCP relay agent.													
ip dhcp snooping information option	Enables the insertion and removal of option-82 information for DHCP packets forwarded without the use of the DHCP relay agent.													
ip dhcp snooping trust	Configures an interface as a trusted source of DHCP messages.													
ip dhcp snooping vlan	Enables DHCP snooping on the specified VLANs.													

Copyright Registration Information	Cisco	Arista														
<div>Copyright Registration Information</div> <div>Cisco NX-OS 6.2</div> <div>Effective date of registration: 11/13/2014</div>	<div><div>ip dhcp snooping information option</div><div><div>To enable the insertion and removal of option-82 information for DHCP packets, use the ip dhcp snooping information option command. To disable the insertion and removal of option-82 information, use the no form of this command.</div><div><div>ip dhcp snooping information option</div><div>no ip dhcp snooping information option</div></div></div><div><div>Syntax Description</div><div>This command has no arguments or keywords.</div></div><div><div>Defaults</div><div>By default, the device does not insert and remove option-82 information.</div></div><div><div>Command Modes</div><div>Global configuration</div></div><div><div>Supported User Roles</div><div>network-admin vdc-admin</div></div><div><div>Command History</div><table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.0(1)</td><td>This command was introduced.</td></tr></table></div><div><div>Usage Guidelines</div><div>To use this command, you must enable the DHCP snooping feature (see the feature dhcp command). This command does not require a license.</div></div><div><div>Examples</div><div><div>This example shows how to globally enable DHCP snooping:</div><div>switch# configure terminal switch(config)# ip dhcp snooping information option switch(config)#</div></div></div><div><div>Related Commands</div><table><tr><th>Command</th><th>Description</th></tr><tr><td>ip dhcp relay information option</td><td>Enables the insertion and removal of option-82 information from DHCP packets forwarded by the DHCP relay agent.</td></tr><tr><td>ip dhcp snooping</td><td>Globally enables DHCP snooping on the device.</td></tr><tr><td>ip dhcp snooping trust</td><td>Configures an interface as a trusted source of DHCP messages.</td></tr><tr><td>ip dhcp snooping vlan</td><td>Enables DHCP snooping on the specified VLANs.</td></tr></table></div></div>	Release	Modification	4.0(1)	This command was introduced.	Command	Description	ip dhcp relay information option	Enables the insertion and removal of option-82 information from DHCP packets forwarded by the DHCP relay agent.	ip dhcp snooping	Globally enables DHCP snooping on the device.	ip dhcp snooping trust	Configures an interface as a trusted source of DHCP messages.	ip dhcp snooping vlan	Enables DHCP snooping on the specified VLANs.	<div><div>ip dhcp snooping information option</div><div><div>The ip dhcp snooping information option command enables the insertion of option-82 DHCP snooping information in DHCP packets on VLANs where DHCP snooping is enabled. DHCP snooping is a layer 2 switch process that allows relay agents to provide remote-ID and circuit-ID information to DHCP reply and request packets. DHCP servers use this information to determine the originating port of DHCP requests and associate a corresponding IP address to that port.</div><div>DHCP snooping uses information option (Option-82) to include the switch MAC address (router-ID) along with the physical interface name and VLAN number (circuit-ID) in DHCP packets. After adding the information to the packet, the DHCP relay agent forwards the packet to the DHCP server through DHCP protocol processes.</div><div>VLAN snooping on a specified VLAN requires each of these conditions:</div><div><div><div><div></div></div><div>DHCP snooping is globally enabled.</div></div><div><div><div></div></div><div>Insertion of option-82 information in DHCP packets is enabled.</div></div><div><div><div></div></div><div>DHCP snooping is enabled on the specified VLAN.</div></div><div><div><div></div></div><div>DHCP relay is enabled on the corresponding VLAN interface.</div></div></div><div>When global DHCP snooping is not enabled, the ip dhcp snooping information option command persists in running-config without any operational effect.</div><div>The no ip dhcp snooping information option and default ip dhcp snooping information option commands disable the insertion of option-82 DHCP snooping information in DHCP packets by removing the ip dhcp snooping information option statement from running-config.</div><div><div><div>Platform</div>Trident</div><div><div>Command Mode</div>Global Configuration</div></div><div><div>Command Syntax</div><div><div>ip dhcp snooping information option</div><div>no ip dhcp snooping information option</div><div>default ip dhcp snooping information option</div></div></div><div><div>Related Commands</div><div><div><div></div><div>ip dhcp snooping</div><div>globally enables DHCP snooping.</div></div><div><div><div></div><div>ip dhcp snooping vlan</div><div>enables DHCP snooping on specified VLANs.</div></div><div><div><div></div><div>ip helper-address</div><div>enables the DHCP relay agent on a configuration mode interface.</div></div></div></div><div><div>Example</div><div><div><div></div><div>These commands enable DHCP snooping on DHCP packets from ports on snooping-enabled VLANs. DHCP snooping was previously enabled on the switch.</div></div><div><div>switch(config)#ip dhcp snooping information option switch(config)#show ip dhcp snooping DHCP Snooping is enabled DHCP Snooping is operational DHCP Snooping is configured on following VLANs: 100 DHCP Snooping is operational on following VLANs: 100 Insertion of Option-82 is enabled Circuit-id format: Interface name:Vlan ID Remote-id: 00:1c:73:1f:b4:38 (Switch MAC) switch(config)#</div></div></div></div></div></div></div></div>
	Release	Modification														
	4.0(1)	This command was introduced.														
	Command	Description														
	ip dhcp relay information option	Enables the insertion and removal of option-82 information from DHCP packets forwarded by the DHCP relay agent.														
	ip dhcp snooping	Globally enables DHCP snooping on the device.														
	ip dhcp snooping trust	Configures an interface as a trusted source of DHCP messages.														
	ip dhcp snooping vlan	Enables DHCP snooping on the specified VLANs.														

Copyright Registration Information	Cisco	Arista																					
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<table><tr><th>Related Commands</th><th>Command</th><th>Description</th></tr><tr><td></td><td>ip dhcp snooping</td><td>Globally enables DHCP snooping on the device.</td></tr><tr><td></td><td>ip dhcp snooping information option</td><td>Enables the insertion and removal of Option-82 information for DHCP packets forwarded without the use of the DHCP relay agent.</td></tr><tr><td></td><td>ip dhcp snooping verify mac-address</td><td>Enables MAC address verification as part of DHCP snooping.</td></tr><tr><td></td><td>ip dhcp snooping vlan</td><td>Enables DHCP snooping on the specified VLANs.</td></tr><tr><td></td><td>show ip dhcp snooping</td><td>Displays general information about DHCP snooping.</td></tr><tr><td></td><td>show running-config dhcp</td><td>Displays DHCP snooping configuration, including IP Source Guard configuration.</td></tr></table> Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-328.	Related Commands	Command	Description		ip dhcp snooping	Globally enables DHCP snooping on the device.		ip dhcp snooping information option	Enables the insertion and removal of Option-82 information for DHCP packets forwarded without the use of the DHCP relay agent.		ip dhcp snooping verify mac-address	Enables MAC address verification as part of DHCP snooping.		ip dhcp snooping vlan	Enables DHCP snooping on the specified VLANs.		show ip dhcp snooping	Displays general information about DHCP snooping.		show running-config dhcp	Displays DHCP snooping configuration, including IP Source Guard configuration.	<div>ip dhcp snooping vlan</div> <p>The ip dhcp snooping vlan command enables DHCP snooping on specified VLANs. DHCP snooping is a layer 2 process that allows relay agents to provide remote-ID and circuit-ID information in DHCP packets. DHCP servers use this data to determine the originating port of DHCP requests and associate a corresponding IP address to that port. DHCP snooping is configured on a global and VLAN basis.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1271.</p>
Related Commands	Command	Description																					
	ip dhcp snooping	Globally enables DHCP snooping on the device.																					
	ip dhcp snooping information option	Enables the insertion and removal of Option-82 information for DHCP packets forwarded without the use of the DHCP relay agent.																					
	ip dhcp snooping verify mac-address	Enables MAC address verification as part of DHCP snooping.																					
	ip dhcp snooping vlan	Enables DHCP snooping on the specified VLANs.																					
	show ip dhcp snooping	Displays general information about DHCP snooping.																					
	show running-config dhcp	Displays DHCP snooping configuration, including IP Source Guard configuration.																					
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<table><tr><th>Command</th><th>Description</th></tr><tr><td>ip dhcp snooping trust</td><td>Configures an interface as a trusted source of DHCP messages.</td></tr><tr><td>ip dhcp snooping vlan</td><td>Enables DHCP snooping on the specified VLANs.</td></tr><tr><td>show ip dhcp snooping</td><td>Displays general information about DHCP snooping.</td></tr><tr><td>show running-config dhcp</td><td>Displays DHCP snooping configuration, including IP Source Guard configuration.</td></tr></table> Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-330.	Command	Description	ip dhcp snooping trust	Configures an interface as a trusted source of DHCP messages.	ip dhcp snooping vlan	Enables DHCP snooping on the specified VLANs.	show ip dhcp snooping	Displays general information about DHCP snooping.	show running-config dhcp	Displays DHCP snooping configuration, including IP Source Guard configuration.	<p>Related Commands</p> <ul style="list-style-type: none">ip dhcp snooping globally enables DHCP snooping.ip dhcp snooping vlan enables DHCP snooping on specified VLANs.ip dhcp snooping information option enables insertion of option-82 snooping data.ip helper-address enables the DHCP relay agent on a configuration mode interface. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1302.</p>											
Command	Description																						
ip dhcp snooping trust	Configures an interface as a trusted source of DHCP messages.																						
ip dhcp snooping vlan	Enables DHCP snooping on the specified VLANs.																						
show ip dhcp snooping	Displays general information about DHCP snooping.																						
show running-config dhcp	Displays DHCP snooping configuration, including IP Source Guard configuration.																						

Copyright Registration Information	Cisco	Arista																																				
<div>Copyright Registration Information</div> <div>Cisco NX-OS 6.2</div> <div>Effective date of registration: 11/13/2014</div>	<div><div>ip dhcp snooping vlan</div><div><div>To enable DHCP snooping on one or more VLANs, use the ip dhcp snooping vlan command. To disable DHCP snooping on one or more VLANs, use the no form of this command.</div><div><div>ip dhcp snooping vlan vlan-list</div><div>no ip dhcp snooping vlan vlan-list</div></div></div><table><tr><td>Syntax Description</td><td>vlan-list</td><td>Range of VLANs on which to enable DHCP snooping. The vlan-list argument allows you to specify a single VLAN ID, a range of VLAN IDs, or comma-separated IDs and ranges (see the "Examples" section). Valid VLAN IDs are from 1 to 4096.</td></tr><tr><td>Defaults</td><td colspan="2">By default, DHCP snooping is not enabled on any VLAN.</td></tr><tr><td>Command Modes</td><td colspan="2">Global configuration</td></tr><tr><td>Supported User Roles</td><td colspan="2">network-admin vdc-admin</td></tr><tr><td>Command History</td><td>Release</td><td>Modification</td></tr><tr><td></td><td>4.0(1)</td><td>This command was introduced.</td></tr><tr><td>Usage Guidelines</td><td colspan="2">To use this command, you must enable the DHCP snooping feature (see the feature dhcp command). This command does not require a license.</td></tr><tr><td>Examples</td><td colspan="2">This example shows how to enable DHCP snooping on VLANs 100, 200, and 250 through 252: switch# configure terminal switch(config)# ip dhcp snooping vlan 100,200,250-252 switch(config)#</td></tr><tr><td>Related Commands</td><td>Command</td><td>Description</td></tr><tr><td></td><td>ip dhcp snooping</td><td>Globally enables DHCP snooping on the device.</td></tr><tr><td></td><td>ip dhcp snooping information option</td><td>Enables the insertion and removal of option-82 information for DHCP packets forwarded without the use of the DHCP relay agent.</td></tr><tr><td></td><td>ip dhcp snooping trust</td><td>Configures an interface as a trusted source of DHCP messages.</td></tr></table></div>	Syntax Description	vlan-list	Range of VLANs on which to enable DHCP snooping. The vlan-list argument allows you to specify a single VLAN ID, a range of VLAN IDs, or comma-separated IDs and ranges (see the "Examples" section). Valid VLAN IDs are from 1 to 4096.	Defaults	By default, DHCP snooping is not enabled on any VLAN.		Command Modes	Global configuration		Supported User Roles	network-admin vdc-admin		Command History	Release	Modification		4.0(1)	This command was introduced.	Usage Guidelines	To use this command, you must enable the DHCP snooping feature (see the feature dhcp command). This command does not require a license.		Examples	This example shows how to enable DHCP snooping on VLANs 100, 200, and 250 through 252: switch# configure terminal switch(config)# ip dhcp snooping vlan 100,200,250-252 switch(config)#		Related Commands	Command	Description		ip dhcp snooping	Globally enables DHCP snooping on the device.		ip dhcp snooping information option	Enables the insertion and removal of option-82 information for DHCP packets forwarded without the use of the DHCP relay agent.		ip dhcp snooping trust	Configures an interface as a trusted source of DHCP messages.	<div><div>ip dhcp snooping vlan</div><div><div>The ip dhcp snooping vlan command enables DHCP snooping on specified VLANs. DHCP snooping is a layer 2 process that allows relay agents to provide remote-ID and circuit-ID information in DHCP packets. DHCP servers use this data to determine the originating port of DHCP requests and associate a corresponding IP address to that port. DHCP snooping is configured on a global and VLAN basis.</div><div>VLAN snooping on a specified VLAN requires each of these conditions:<ul style="list-style-type: none">DHCP snooping is globally enabled.Insertion of option-82 information in DHCP packets is enabled.DHCP snooping is enabled on the specified VLAN.DHCP relay is enabled on the corresponding VLAN interface.</div><div>When global DHCP snooping is not enabled, the ip dhcp snooping vlan command persists in running-config without any operational affect.</div><div>The no ip dhcp snooping information option and default ip dhcp snooping information option commands disable DHCP snooping operability by removing the ip dhcp snooping information option statement from running-config.</div><div><div>Platform</div><div>Trident</div><div>Command Mode</div><div>Global Configuration</div></div><div><div>Command Syntax</div><div><div>ip dhcp snooping vlan v_range</div><div>no ip dhcp snooping vlan v_range</div><div>default ip dhcp snooping vlan v_range</div></div><div><div>Parameters</div><div><ul style="list-style-type: none">v_range VLANs upon which snooping is enabled. Formats include a number, a number range, or a comma-delimited list of numbers and ranges. Numbers range from 1 to 4094.</div><div><div>Related Commands</div><div><ul style="list-style-type: none">ip dhcp snooping globally enables DHCP snooping.ip dhcp snooping information option enables insertion of option-82 snooping data.ip helper-address enables the DHCP relay agent on a configuration mode interface.</div><div><div>Example</div><div><ul style="list-style-type: none">These commands enable DHCP snooping globally, DHCP on VLAN interface 100, and DHCP snooping on VLAN 100.<pre>switch(config)#ip dhcp snooping switch(config)#ip dhcp snooping information option switch(config)#ip dhcp snooping vlan 100 switch(config)#interface vlan 100 switch(config-if-Vl100)#ip helper-address 10.4.4.4 switch(config-if-Vl100)#show ip dhcp snooping DHCP Snooping is enabled DHCP Snooping is operational DHCP Snooping is configured on following VLANs: 100 DHCP Snooping is operational on following VLANs: 100 Insertion of Option-82 is enabled Circuit-id format: Interface name:Vlan ID Remote-id: 00:1c:73:1f:b4:38 (Switch MAC) switch(config)#</pre></div></div></div></div></div></div></div>
	Syntax Description	vlan-list	Range of VLANs on which to enable DHCP snooping. The vlan-list argument allows you to specify a single VLAN ID, a range of VLAN IDs, or comma-separated IDs and ranges (see the "Examples" section). Valid VLAN IDs are from 1 to 4096.																																			
	Defaults	By default, DHCP snooping is not enabled on any VLAN.																																				
	Command Modes	Global configuration																																				
	Supported User Roles	network-admin vdc-admin																																				
	Command History	Release	Modification																																			
		4.0(1)	This command was introduced.																																			
	Usage Guidelines	To use this command, you must enable the DHCP snooping feature (see the feature dhcp command). This command does not require a license.																																				
	Examples	This example shows how to enable DHCP snooping on VLANs 100, 200, and 250 through 252: switch# configure terminal switch(config)# ip dhcp snooping vlan 100,200,250-252 switch(config)#																																				
	Related Commands	Command	Description																																			
	ip dhcp snooping	Globally enables DHCP snooping on the device.																																				
	ip dhcp snooping information option	Enables the insertion and removal of option-82 information for DHCP packets forwarded without the use of the DHCP relay agent.																																				
	ip dhcp snooping trust	Configures an interface as a trusted source of DHCP messages.																																				

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p><code>set-dscp-transmit dscp-value</code> Specifies the differentiated services code point (DSCP) value for IPv4 and IPv6 packets. The range is from 0 to 63.</p> <p>Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-444.</p>	<p>qos dscp</p> <p>The <code>qos dscp</code> command specifies the default differentiated services code point (DSCP) value of the configuration mode interface. The default DSCP determines the traffic class for non-IP packets that are inbound on DSCP trusted ports. DSCP trusted ports determine the traffic class for inbound packets as follows:</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1093.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 991; Arista User Manual, v. 4.11.1 (1/11/13), at 795; Arista User Manual v. 4.10.3 (10/22/12), at 646; Arista User Manual v. 4.9.3.2 (5/3/12), at 576; Arista User Manual v. 4.8.2 (11/18/11), at 666.</p>

Copyright Registration Information	Cisco	Arista
<div>Cisco NX-OS 6.2</div> <div>Effective date of registration: 11/13/2014</div>	<div><div>policy-map type control-plane</div><div>To create or specify a control plane policy map and enter policy map configuration mode, use the <code>policy-map type control-plane</code> command. To delete a control plane policy map, use the <code>no</code> form of this command.</div><div><div>policy-map type control-plane</div>policy-map-name</div><div>no policy-map type control-planepolicy-map-name</div><div><div>Syntax Description</div><div>policy-map-name</div><div>Name of the class map. The name is alphanumeric, case sensitive, and has a maximum of 64 characters.</div></div><div><div>Defaults</div><div>None</div></div><div><div>Command Modes</div><div>Global configuration</div></div><div><div>SupportedUserRoles</div><div>network-admin</div><div>vdc-admin</div></div><div><div>Command History</div><div><div>Release</div><div>Modification</div></div><div><div>4.0(1)</div><div>This command was introduced.</div></div></div><div><div>Usage Guidelines</div><div>You can use this command only in the default VDC.</div><div>This command does not require a license.</div></div><div><div>Examples</div><div>This example shows how to specify a control plane policy map and enter policy map configuration mode:</div><div>switch# config t</div><div>switch(config)# policy-map type control-plane PolicyMapA</div><div>switch(config-pmap)#</div><div>This example shows how to delete a control plane policy map:</div><div>switch# config t</div><div>switch(config)# no policy-map type control-plane PolicyMapA</div></div></div> <div>Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-448.</div>	<div><div>policy-map type control-plane</div><div>The <code>policy-map type control-plane</code> command places the switch in Policy-Map (control plane) configuration mode, which is a group change mode that modifies a control-plane policy map. A policy map is a data structure that consists of class maps that identify a specific data stream and specify bandwidth and shaping parameters that controls its transmission. Control plane policy maps are applied to the control plane to manage traffic.</div><div>The <code>copp-system-policy</code> policy map is supplied with the switch and is always applied to the control plane. <code>Copp-system-policy</code> is the only valid control plane policy map.</div><div>The <code>exit</code> command saves pending policy map changes to <i>running-config</i> and returns the switch to global configuration mode. Policy map changes are also saved by entering a different configuration mode. The <code>abort</code> command discards pending changes, returning the switch to global configuration mode.</div><div>The <code>no policy-map type control-plane</code> and <code>default policy-map type control-plane</code> commands delete the specified policy map by removing the corresponding <code>policy-map type control-plane</code> command and its associated configuration.</div><div><div>Platform</div><div>FM6000, Petra, Trident</div></div><div><div>Command Mode</div><div>Global Configuration</div></div><div><div>Command Syntax</div><div><div>policy-map type control-plane</div> copp-system-policy</div><div>no policy-map type control-plane copp-system-policy</div><div>default policy-map type control-plane copp-system-policy</div><div>copp-system-policy is supplied with the switch and is the only valid control plane policy map.</div></div><div><div>Commands Available in Policy-Map Configuration Mode</div><div><div>class (policy-map (control-plane) - FM6000)</div><div>class (policy-map (control-plane) - Trident)</div></div></div><div><div>Related Commands</div><div><div>class-map type control-plane</div> enters control-plane class-map configuration mode.</div></div><div><div>Example</div><div>This command places the switch in policy-map configuration mode to edit the <code>copp-system-policy</code> policy map.</div><div><div>switch(config)#policy-map type control-plane</div> copp-system-policy</div><div>switch(config-pmap-copp-system-policy)#</div></div></div> <div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1194.</div> <div>See also Arista User Manual v. 4.12.3 (7/17/13), at 980; Arista User Manual, v. 4.11.1 (1/11/13), at 784.</div>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>To view per-entry statistics, use the <code>show access-lists</code> command or the applicable following command:</p> <ul style="list-style-type: none"> • <code>show ip access-lists</code> • <code>show ipv6 access-lists</code> • <code>show mac access-lists</code> <p>Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-517.</p>	<p>Displaying Contents of an ACL</p> <p>These commands display ACL contents.</p> <ul style="list-style-type: none"> • <code>show ip access-lists</code> • <code>show ipv6 access-lists</code> • <code>show mac access-lists</code> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 845.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 724; Arista User Manual, v. 4.11.1 (1/11/13), at 552; Arista User Manual v. 4.10.3 (10/22/12), at 466.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>Examples</p> <p>This example shows how to display control plane class map information:</p> <pre>switch# show class-map type control-plane</pre> <pre>class-map type control-plane match-any copp-system-class-critical match access-grp name copp-system-acl-arp match access-grp name copp-system-acl-msdp class-map type control-plane match-any copp-system-class-important match access-grp name copp-system-acl-gre match access-grp name copp-system-acl-tacas class-map type control-plane match-any copp-system-class-normal match access-grp name copp-system-acl-icmp match redirect dhcp-snoop match redirect arp-inspect match exception ip option match exception ip icmp redirect match exception ip icmp unreachable</pre> <p>Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-552.</p>	<p>Example</p> <ul style="list-style-type: none"> • This command displays all control plane class maps. • This command displays the available control plane class maps. <pre>switch>show class-map type control-plane</pre> <pre>Class-map: CM-CP1 (match-any) Match: ip access-group name LIST-CP1 Class-map: copp-system-aclog (match-any) Class-map: copp-system-arp (match-any) Class-map: copp-system-arpresolver (match-any) Class-map: copp-system-bpdu (match-any) Class-map: copp-system-glean (match-any) Class-map: copp-system-igmp (match-any) Class-map: copp-system-ipmcmiss (match-any) Class-map: copp-system-ipmcsvd (match-any) Class-map: copp-system-l3destmiss (match-any) Class-map: copp-system-l3slowpath (match-any) Class-map: copp-system-l3ttl1 (match-any) Class-map: copp-system-lacp (match-any) Class-map: copp-system-lldp (match-any) Class-map: copp-system-selfip (match-any) Class-map: copp-system-selfip-tc6to7 (match-any) Class-map: copp-system-sflow (match-any) Class-map: copp-system-tc3to5 (match-any) Class-map: copp-system-tc6to7 (match-any)</pre> <p>switch></p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/20140), at 1212.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>Examples</p> <p>This example shows how to display the DHCP relay status and configured DHCP server addresses:</p> <pre>switch# show ip dhcp relay DHCP relay service is enabled Insertion of option 82 is enabled Insertion of VRF suboptions is enabled Helper addresses are configured on the following interfaces: Interface Relay Address VRF Name ----- Ethernet1/4 10.10.10.1 red switch#</pre> <p>Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-630.</p>	<p>Example</p> <ul style="list-style-type: none"> This command displays the DHCP relay agent configuration status. <pre>switch>show ip dhcp relay DHCP servers: 172.22.22.11 Vlan1000: DHCP clients are permitted on this interface</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1237.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1047; Arista User Manual, v. 4.11.1 (1/11/13), at 868; Arista User Manual v. 4.10.3 (10/22/12), at 716.</p>
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>Examples</p> <p>This example shows how to display general status information about DHCP snooping:</p> <pre>switch# show ip dhcp snooping DHCP snooping service is enabled Switch DHCP snooping is enabled DHCP snooping is configured on the following VLANs: 1,13 DHCP snooping is operational on the following VLANs: 1 Insertion of Option 82 is disabled Verification of MAC address is enabled DHCP snooping trust is configured on the following interfaces: Interface trusted ----- Ethernet2/3 yes switch#</pre> <p>Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-634.</p>	<p>Example</p> <ul style="list-style-type: none"> This command DHCP snooping hardware status. <pre>switch>show ip dhcp snooping hardware DHCP Snooping is enabled DHCP Snooping is enabled on following VLANs: None Vlans enabled per Slice Slice: FixedSystem None switch></pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1304.</p>

Copyright Registration Information	Cisco	Arista																																			
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<div>Examples</div> <div>This example shows how to use the <code>show port-security</code> command to view the status of the port security feature on a device:</div> <div>switch# show port-security</div> <div>Total Secured Mac Addresses in System (excluding one mac per port) : 0 Max Addresses limit in System (excluding one mac per port) : 8192</div> <div><table><thead><tr><th>Secure Port</th><th>MaxSecureAddr (Count)</th><th>CurrentAddr (Count)</th><th>SecurityViolation (Count)</th><th>Security Action</th></tr></thead><tbody><tr><td>Ethernet1/1</td><td>5</td><td>1</td><td>0</td><td>Shutdown</td></tr></tbody></table></div> <div>switch#</div> <div>Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-661.</div>	Secure Port	MaxSecureAddr (Count)	CurrentAddr (Count)	SecurityViolation (Count)	Security Action	Ethernet1/1	5	1	0	Shutdown	<div>Example</div> <div><ul style="list-style-type: none">These commands enable MAC security on Ethernet interface 7, set the maximum number of assigned MAC addresses to 2, assigns two static MAC addresses to the interface, and clears the dynamic MAC addresses for the interface.</div> <div>switch(config)#interface ethernet 7 switch(config-if-Et7)#switchport port-security switch(config-if-Et7)#switchport port-security maximum 2 switch(config-if-Et7)#exit switch(config)#mac address-table static 0034.24c2.8f11 vlan 10 interface ethernet 7 switch(config)#mac address-table static 4464.842d.17ce vlan 10 interface ethernet 7 switch(config)#clear mac address-table dynamic interface ethernet 7 switch(config)#show port-security</div> <div><table><thead><tr><th>Secure Port</th><th>MaxSecureAddr (Count)</th><th>CurrentAddr (Count)</th><th>SecurityViolation (Count)</th><th>Security Action</th></tr></thead><tbody><tr><td>Et7</td><td>2</td><td>2</td><td>0</td><td>Shutdown</td></tr></tbody></table></div> <div>Total Addresses in System: 1 switch(config)#show port-security address</div> <div>Secure Mac Address Table</div> <div><table><thead><tr><th>Vlan</th><th>Mac Address</th><th>Type</th><th>Ports</th><th>Remaining Age (mins)</th></tr></thead><tbody><tr><td>10</td><td>0034.24c2.8f11</td><td>SecureConfigured</td><td>Et7</td><td>N/A</td></tr><tr><td>10</td><td>4464.842d.17ce</td><td>SecureConfigured</td><td>Et7</td><td>N/A</td></tr></tbody></table></div> <div>Total Mac Addresses for this criterion: 2 switch(config)#</div> <div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 632.</div> <div>See also Arista User Manual v. 4.13.6F (4/14/2014), at 624; Arista User Manual v. 4.12.3 (7/17/13), at 501; Arista User Manual, v. 4.11.1 (1/11/13), at 405-06; Arista User Manual v. 4.10.3 (10/22/12), at 336; Arista User Manual v. 4.9.3.2 (5/3/12), at 405-06.</div>	Secure Port	MaxSecureAddr (Count)	CurrentAddr (Count)	SecurityViolation (Count)	Security Action	Et7	2	2	0	Shutdown	Vlan	Mac Address	Type	Ports	Remaining Age (mins)	10	0034.24c2.8f11	SecureConfigured	Et7	N/A	10	4464.842d.17ce	SecureConfigured	Et7	N/A
	Secure Port	MaxSecureAddr (Count)	CurrentAddr (Count)	SecurityViolation (Count)	Security Action																																
Ethernet1/1	5	1	0	Shutdown																																	
Secure Port	MaxSecureAddr (Count)	CurrentAddr (Count)	SecurityViolation (Count)	Security Action																																	
Et7	2	2	0	Shutdown																																	
Vlan	Mac Address	Type	Ports	Remaining Age (mins)																																	
10	0034.24c2.8f11	SecureConfigured	Et7	N/A																																	
10	4464.842d.17ce	SecureConfigured	Et7	N/A																																	

Copyright Registration Information	Cisco	Arista																																																												
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<p>Examples</p> <p>This example shows how to use the <code>show port-security address</code> command to view information about all MAC addresses secured by port security:</p> <pre>switch# show port-security address</pre> <p>Total Secured Mac Addresses in System (excluding one mac per port) : 0 Max Addresses limit in System (excluding one mac per port) : 8192</p> <table><tr><th colspan="5">Secure Mac Address Table</th></tr><tr><th>Vlan</th><th>Mac Address</th><th>Type</th><th>Ports</th><th>Remaining Age (mins)</th></tr><tr><td>1</td><td>0054.AAB3.770F</td><td>STATIC</td><td>port-channel1</td><td>0</td></tr><tr><td>1</td><td>00EE.378A.ABCE</td><td>STATIC</td><td>Ethernet1/4</td><td>0</td></tr></table> <pre>switch#</pre> <p>This example shows how to use the <code>show port-security address</code> command to view the MAC addresses secured by the port security feature on the Ethernet 1/4 interface:</p> <pre>switch# show port-security address interface ethernet 1/4</pre> <table><tr><th colspan="5">Secure Mac Address Table</th></tr><tr><th>Vlan</th><th>Mac Address</th><th>Type</th><th>Ports</th><th>Remaining Age (mins)</th></tr><tr><td>1</td><td>00EE.378A.ABCE</td><td>STATIC</td><td>Ethernet1/4</td><td>0</td></tr></table> <pre>switch#</pre> <p>Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-664.</p>	Secure Mac Address Table					Vlan	Mac Address	Type	Ports	Remaining Age (mins)	1	0054.AAB3.770F	STATIC	port-channel1	0	1	00EE.378A.ABCE	STATIC	Ethernet1/4	0	Secure Mac Address Table					Vlan	Mac Address	Type	Ports	Remaining Age (mins)	1	00EE.378A.ABCE	STATIC	Ethernet1/4	0	<p>Example</p> <ul style="list-style-type: none">This command displays MAC addresses assigned to port-security protected interfaces. <pre>switch>show port-security address</pre> <table><tr><th colspan="5">Secure Mac Address Table</th></tr><tr><th>Vlan</th><th>Mac Address</th><th>Type</th><th>Ports</th><th>Remaining Age (mins)</th></tr><tr><td>10</td><td>164f.29ae.4e14</td><td>SecureConfigured</td><td>Et7</td><td>N/A</td></tr><tr><td>10</td><td>164f.29ae.4f11</td><td>SecureConfigured</td><td>Et7</td><td>N/A</td></tr><tr><td>10</td><td>164f.320a.3a11</td><td>SecureConfigured</td><td>Et7</td><td>N/A</td></tr></table> <p>Total Mac Addresses for this criterion: 3</p> <pre>switch></pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 698.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 562; Arista User Manual, v. 4.11.1 (1/11/13), at 446; Arista User Manual v. 4.10.3 (10/22/12), at 366; Arista User Manual v. 4.9.3.2 (5/3/12), at 338.</p>	Secure Mac Address Table					Vlan	Mac Address	Type	Ports	Remaining Age (mins)	10	164f.29ae.4e14	SecureConfigured	Et7	N/A	10	164f.29ae.4f11	SecureConfigured	Et7	N/A	10	164f.320a.3a11	SecureConfigured	Et7	N/A
	Secure Mac Address Table																																																													
Vlan	Mac Address	Type	Ports	Remaining Age (mins)																																																										
1	0054.AAB3.770F	STATIC	port-channel1	0																																																										
1	00EE.378A.ABCE	STATIC	Ethernet1/4	0																																																										
Secure Mac Address Table																																																														
Vlan	Mac Address	Type	Ports	Remaining Age (mins)																																																										
1	00EE.378A.ABCE	STATIC	Ethernet1/4	0																																																										
Secure Mac Address Table																																																														
Vlan	Mac Address	Type	Ports	Remaining Age (mins)																																																										
10	164f.29ae.4e14	SecureConfigured	Et7	N/A																																																										
10	164f.29ae.4f11	SecureConfigured	Et7	N/A																																																										
10	164f.320a.3a11	SecureConfigured	Et7	N/A																																																										
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<p>Related Commands</p> <table><tr><th>Command</th><th>Description</th></tr><tr><td><code>feature dhcp</code></td><td>Enables the DHCP snooping feature on the device.</td></tr><tr><td><code>ip dhcp snooping</code></td><td>Globally enables DHCP snooping on the device.</td></tr><tr><td><code>service dhcp</code></td><td>Enables or disables the DHCP relay agent.</td></tr><tr><td><code>show ip dhcp snooping</code></td><td>Displays general information about DHCP snooping.</td></tr><tr><td><code>show ip dhcp snooping binding</code></td><td>Displays IP-MAC address bindings, including the static IP source entries.</td></tr></table> <p>Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-695.</p>	Command	Description	<code>feature dhcp</code>	Enables the DHCP snooping feature on the device.	<code>ip dhcp snooping</code>	Globally enables DHCP snooping on the device.	<code>service dhcp</code>	Enables or disables the DHCP relay agent.	<code>show ip dhcp snooping</code>	Displays general information about DHCP snooping.	<code>show ip dhcp snooping binding</code>	Displays IP-MAC address bindings, including the static IP source entries.	<p>ip dhcp snooping</p> <p>The <code>ip dhcp snooping</code> command enables DHCP snooping globally on the switch. DHCP snooping is a set of layer 2 processes that can be configured on LAN switches and used with DHCP servers to control network access to clients with specific IP/MAC addresses. The switch supports Option-82 insertion, which is a DHCP snooping process that allows relay agents to provide remote-ID and circuit-ID information to DHCP reply and request packets. DHCP servers use this information to determine the originating port of DHCP requests and associate a corresponding IP address to that port. DHCP servers use port information to track host location and IP address usage by authorized physical ports.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1269.</p>																																																
Command	Description																																																													
<code>feature dhcp</code>	Enables the DHCP snooping feature on the device.																																																													
<code>ip dhcp snooping</code>	Globally enables DHCP snooping on the device.																																																													
<code>service dhcp</code>	Enables or disables the DHCP relay agent.																																																													
<code>show ip dhcp snooping</code>	Displays general information about DHCP snooping.																																																													
<code>show ip dhcp snooping binding</code>	Displays IP-MAC address bindings, including the static IP source entries.																																																													

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>Usage Guidelines In order for LLDP to discover servers connected to your device, the servers must be running openLLDP software.</p> <p>LLDP must be enabled on the device before you can enable or disable it on any interfaces.</p> <p>Note LLDP is supported only on physical interfaces. LLDP timers and type, length, and value (TLV) descriptions cannot be configured using Cisco DCNM.</p> <p>LLDP can discover up to one device per port. LLDP can discover up to one server per port. LLDP can discover only Linux servers that are connected to your device. LLDP can discover Linux servers, if they are not using a converged network adapter (CNA); however, LLDP cannot discover other types of servers.</p> <p>Make sure that you are in the correct virtual device context (VDC). To switch VDCs, use the <code>switchto vdc</code> command.</p> <p>This command does not require a license.</p> <p>Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 174.</p>	<p>12.2.4 Guidelines and Limitations</p> <p>LLDP has the following configuration guidelines and limitations:</p> <ul style="list-style-type: none"> • LLDP must be enabled on the device before you can enable or disable it on any interface. • LLDP is supported only on physical interfaces. • LLDP can discover up to one device per port. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 576.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 448; Arista User Manual, v. 4.11.1 (1/11/13), at 366.</p>

Copyright Registration Information	Cisco	Arista
<div>Cisco NX-OS 6.2</div> <div>Effective date of registration: 11/13/2014</div>	<div><div>lldp holdtime</div><div><div>To configure the amount of time that a receiving device should hold the information sent by your device before discarding it, use the lldp holdtime command. To remove the hold time configuration, use the no form of this command.</div><div>lldp holdtime seconds</div></div><div><div>Syntax Description</div><div>secondsHold time in seconds. The range is from 10 to 255 seconds.</div></div><div><div>Defaults</div><div>120 seconds</div></div><div><div>Command Modes</div><div>Global configuration mode (config)</div></div><div><div>Supported User Roles</div><div>network-admin network-operator vdc-admin vdc-operator</div></div><div><div>Command History</div><div><div>Release</div><div>Modification</div><div>5.0(1)</div><div>This command was introduced.</div></div></div><div><div>Usage Guidelines</div><div><div>Make sure that you are in the correct virtual device context (VDC). To switch VDCs, use the switchto vdc command.</div><div>This command does not require a license.</div></div></div><div><div>Examples</div><div><div>This example shows how to configure the Link Layer Discovery Protocol (LLDP) hold time:</div><div>switch(config)# lldp holdtime 180 switch(config)#</div><div>This example shows how to remove the LLDP hold time configuration:</div><div>switch(config)# no lldp holdtime 180 switch(config)#</div></div></div></div>	<div><div>lldp holdtime</div><div><div>The lldp holdtime command specifies the amount of time a receiving device should hold the information sent by the device before discarding it.</div><div><div>Platformall</div><div>Command ModeGlobal Configuration</div></div><div><div>Command Syntax</div><div>lldp holdtime period no lldp holdtime default lldp holdtime</div></div><div><div>Parameters</div><div><div>• period</div><div>The amount of time a receiving device should hold the LLDPDU information sent before discarding it. Value ranges from 10 to 65535 second; default value is 120 seconds.</div></div></div><div><div>Examples</div><div><div>• This command sets the amount of time to 180 seconds before the receiving device discards the LLDPDU information.</div><div>switch(config)# lldp holdtime 180 switch(config)#</div><div>• This command removes the configured time before the receiving device discards the LLDPDU information.</div><div>switch(config)# no lldp holdtime 180 switch(config)#</div></div></div></div></div>
		<div><div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 585.</div><div><div>See also Arista User Manual v. 4.12.3 (7/17/13), at 458; Arista User Manual, v. 4.11.1 (1/11/13), at 376.</div></div></div>

Copyright Registration Information	Cisco	Arista									
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<table border="1"> <tr> <th>Related Commands</th><th>Command</th><th>Description</th></tr> <tr> <td></td><td>lldp reinit</td><td>Specifies the delay time in seconds for LLDP to initialize on any interface.</td></tr> </table> <p>Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 228.</p>	Related Commands	Command	Description		lldp reinit	Specifies the delay time in seconds for LLDP to initialize on any interface.	<p>lldp reinit</p> <p>The lldp reinit command specifies the delay time in seconds for LLDP to initialize on any interface.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 589.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 462; Arista User Manual, v. 4.11.1 (1/11/13), at 380.</p>			
Related Commands	Command	Description									
	lldp reinit	Specifies the delay time in seconds for LLDP to initialize on any interface.									
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<table border="1"> <tr> <th>Related Commands</th><th>Command</th><th>Description</th></tr> <tr> <td></td><td>lldp transmit</td><td>Enables the transmission of LLDP packets on an interface.</td></tr> <tr> <td></td><td>show lldp interface ethernet</td><td>Displays the LLDP configuration on an interface.</td></tr> </table> <p>Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 231.</p>	Related Commands	Command	Description		lldp transmit	Enables the transmission of LLDP packets on an interface.		show lldp interface ethernet	Displays the LLDP configuration on an interface.	<p>lldp transmit</p> <p>The lldp transmit command enables the transmission of LLDP packets on an interface. After you globally enable LLDP, it is enabled on all supported interfaces by default.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 593.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 446; Arista User Manual, v. 4.11.1 (1/11/13), at 384.</p>
Related Commands	Command	Description									
	lldp transmit	Enables the transmission of LLDP packets on an interface.									
	show lldp interface ethernet	Displays the LLDP configuration on an interface.									
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<table border="1"> <tr> <th>Related Commands</th><th>Command</th><th>Description</th></tr> <tr> <td></td><td>lldp holdtime</td><td>Specifies the amount of time in seconds that a receiving device should hold the information sent by your device before discarding it.</td></tr> </table> <p>Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 232.</p>	Related Commands	Command	Description		lldp holdtime	Specifies the amount of time in seconds that a receiving device should hold the information sent by your device before discarding it.	<p>12.3.3.2 Setting the LLDP Hold Time</p> <p>The lldp holdtime command specifies the amount of time in seconds that a receiving device should hold the information sent by the device before discarding it.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 578.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 450; Arista User Manual, v. 4.11.1 (1/11/13), at 368.</p>			
Related Commands	Command	Description									
	lldp holdtime	Specifies the amount of time in seconds that a receiving device should hold the information sent by your device before discarding it.									

Copyright Registration Information	Cisco	Arista												
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<table border="1"> <thead> <tr> <th>Related Commands</th><th>Command</th><th>Description</th></tr> </thead> <tbody> <tr> <td></td><td><code>lldp reinit</code></td><td>Specifies the delay time in seconds for LLDP to initialize on any interface.</td></tr> <tr> <td></td><td><code>lldp holdtime</code></td><td>Specifies the amount of time in seconds that a receiving device should hold the information sent by your device before discarding it.</td></tr> <tr> <td></td><td><code>show lldp timers</code></td><td>Displays the LLDP holdtime, delay time, and update frequency configuration.</td></tr> </tbody> </table> <p>Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 235.</p>	Related Commands	Command	Description		<code>lldp reinit</code>	Specifies the delay time in seconds for LLDP to initialize on any interface.		<code>lldp holdtime</code>	Specifies the amount of time in seconds that a receiving device should hold the information sent by your device before discarding it.		<code>show lldp timers</code>	Displays the LLDP holdtime, delay time, and update frequency configuration.	<p>lldp timer</p> <p>The <code>lldp timer</code> command specifies the amount of time a receiving device should hold the information sent by the device before discarding it. The no form of this command removes the configured LLDP timer.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 591.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 464; Arista User Manual, v. 4.11.1 (1/11/13), at 382.</p>
Related Commands	Command	Description												
	<code>lldp reinit</code>	Specifies the delay time in seconds for LLDP to initialize on any interface.												
	<code>lldp holdtime</code>	Specifies the amount of time in seconds that a receiving device should hold the information sent by your device before discarding it.												
	<code>show lldp timers</code>	Displays the LLDP holdtime, delay time, and update frequency configuration.												
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>lldp tlv-select</p> <p>To configure the type, length, and value (TLV) descriptions to send and receive in Link Layer Discovery Protocol (LLDP) packets, use the <code>lldp tlv-select</code> command. To remove the TLV configuration, use the no form of this command.</p> <p><code>lldp tlv-select [dcbxp management-address port-description port-vlan system-capabilities system-description system-name]</code></p> <p><code>no lldp tlv-select [dcbxp management-address port-description port-vlan system-capabilities system-description system-name]</code></p> <p>Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 236.</p>	<p>12.3.3.5 Selecting the LLDP TLV</p> <p>The <code>lldp tlv-select</code> command configures the type, length, and value (TLV) descriptions to send and receive in Link Layer Discovery Protocol (LLDP) packets. Use the no form of this command to remove the TLV configuration.</p> <p>Example</p> <ul style="list-style-type: none"> This command enables the system descriptions to be included in the TLVs. <pre>switch(config)# lldp tlv-select system-description switch(config)#</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 578.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 465; Arista User Manual, v. 4.11.1 (1/11/13), at 368-69.</p>												

Copyright Registration Information	Cisco	Arista																														
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<h3>logging console</h3> <p>To enable logging messages to the console session, use the logging console command. To disable logging messages to the console session, use the no form of this command.</p> <pre>logging console [severity-level] no logging console</pre> <table border="1"> <tr> <td>Syntax Description</td><td>severity-level</td><td>(Optional) Number of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows:</td></tr> <tr> <td></td><td></td><td> <ul style="list-style-type: none"> 0—emergency: System unusable 1—alert: Immediate action needed 2—critical: Critical condition—default level 3—error: Error condition 4—warning: Warning condition 5—notification: Normal but significant condition 6—informational: Informational message only 7—debugging: Appears during debugging only </td></tr> <tr> <td>Defaults</td><td>None</td><td></td></tr> <tr> <td>Command Modes</td><td>Global configuration mode</td><td></td></tr> <tr> <td>Supported User Roles</td><td>network-admin vdc-admin</td><td></td></tr> <tr> <td>Command History</td><td>Release</td><td>Modification</td></tr> <tr> <td></td><td>4.0(1)</td><td>This command was introduced.</td></tr> <tr> <td>Usage Guidelines</td><td colspan="2">This command does not require a license.</td></tr> <tr> <td>Examples</td><td colspan="2"> <p>This example shows how to enable logging messages with a severity level of 4 (warning) or higher to the console session:</p> <pre>switch# configure terminal switch(config)# logging console 4 switch(config)#</pre> </td></tr> <tr> <td></td><td colspan="2">Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 242.</td></tr> </table>	Syntax Description	severity-level	(Optional) Number of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows:			<ul style="list-style-type: none"> 0—emergency: System unusable 1—alert: Immediate action needed 2—critical: Critical condition—default level 3—error: Error condition 4—warning: Warning condition 5—notification: Normal but significant condition 6—informational: Informational message only 7—debugging: Appears during debugging only 	Defaults	None		Command Modes	Global configuration mode		Supported User Roles	network-admin vdc-admin		Command History	Release	Modification		4.0(1)	This command was introduced.	Usage Guidelines	This command does not require a license.		Examples	<p>This example shows how to enable logging messages with a severity level of 4 (warning) or higher to the console session:</p> <pre>switch# configure terminal switch(config)# logging console 4 switch(config)#</pre>			Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 242.		<h3>logging trap system</h3> <p>The logging trap system command enables the logging of system messages to a remote server, or limits the syslog messages saved to a remote server based on severity. Use this command without a specified level to enable remote logging.</p> <p>The no logging trap system and default logging trap system commands clear the specified method list by removing the corresponding logging trap system command from <i>running-config</i>.</p> <p>Platform all Command Mode Global Configuration</p> <h4>Command Syntax</h4> <pre>logging trap system [FACILITY_LEVEL] [CONDITION] [PROGRAM] [TEXT] no logging trap system [FACILITY_LEVEL] [CONDITION] [PROGRAM] [TEXT] default logging trap system [FACILITY_LEVEL] [CONDITION] [PROGRAM] [TEXT]</pre> <p>The TEXT parameter, when present, is always last. All other parameters can be placed in any order.</p> <h4>Parameters</h4> <ul style="list-style-type: none"> FACILITY_LEVEL Defines the appropriate facility. <ul style="list-style-type: none"> <no parameter> Specifies default facility. facility <facility-name> Specifies named facility. CONDITION Specifies condition level. Options include: <ul style="list-style-type: none"> <no parameter> Specifies default condition level. severity <condition-level> Name of the severity level at which messages should be logged. <p>Valid condition-level options include:</p> <ul style="list-style-type: none"> 0 or emergencies System is unusable 1 or alerts Immediate action needed 2 or critical Critical conditions 3 or errors Error conditions 4 or warnings Warning conditions 5 or notifications Normal but significant conditions 6 or informational Informational messages 7 or debugging Debugging messages <ul style="list-style-type: none"> PROGRAM Filters packets based on program name. Options include: <ul style="list-style-type: none"> <no parameter> All tags or program names. tag program-name Specific tag or program name. TEXT Specifies log message text. Options include: <ul style="list-style-type: none"> <no parameter> Specify text contained in log message. contain reg-expression Specify text contained in log message. <h4>Examples</h4> <ul style="list-style-type: none"> This command enables the logging of system informational messages to a remote server. <pre>switch(config)#logging trap informational switch(config)#</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2015), at 155.</p>
Syntax Description	severity-level	(Optional) Number of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows:																														
		<ul style="list-style-type: none"> 0—emergency: System unusable 1—alert: Immediate action needed 2—critical: Critical condition—default level 3—error: Error condition 4—warning: Warning condition 5—notification: Normal but significant condition 6—informational: Informational message only 7—debugging: Appears during debugging only 																														
Defaults	None																															
Command Modes	Global configuration mode																															
Supported User Roles	network-admin vdc-admin																															
Command History	Release	Modification																														
	4.0(1)	This command was introduced.																														
Usage Guidelines	This command does not require a license.																															
Examples	<p>This example shows how to enable logging messages with a severity level of 4 (warning) or higher to the console session:</p> <pre>switch# configure terminal switch(config)# logging console 4 switch(config)#</pre>																															
	Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 242.																															

Copyright Registration Information	Cisco	Arista															
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>To configure the interval between Precision Time Protocol (PTP) announce messages on an interface or the number of PTP intervals before a timeout occurs on an interface, use the <code>ptp announce</code> command. To remove the interval configuration for PTP messages, use the <code>no</code> form of this command.</p> <p>Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 330.</p>	<p>Set the Peer Delay Request Interval</p> <p>To configure the minimum interval allowed between Precision Time Protocol (PTP) peer delay-request messages, use the <code>ptp pdelay-req interval</code> command.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 273.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 216.</p>															
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>Examples</p> <p>This example shows how to configure the interval between PTP announce messages on an interface:</p> <pre>switch# configure terminal switch(config)# interface ethernet 5/1 switch(config-if)# ptp announce interval 1 switch(config-if)#</pre> <p>Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 330.</p>	<p>Examples</p> <ul style="list-style-type: none"> This command shows how to configure the interval between PTP announce messages on an interface. <pre>switch(config)# interface ethernet 5 switch(config-if-Et5)# ptp announce interval 1 switch(config-if-Et5)#</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 315.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 253; Arista User Manual, v. 4.11.1 (1/11/13), at 199.</p>															
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<table border="1"> <thead> <tr> <th>Related Commands</th><th>Command</th><th>Description</th></tr> </thead> <tbody> <tr> <td></td><td><code>ptp</code></td><td>Enables or disables PTP on an interface.</td></tr> <tr> <td></td><td><code>ptp announce</code></td><td>Configures the interval between PTP announce messages on an interface or the number of PTP intervals before a timeout occurs on an interface.</td></tr> <tr> <td></td><td><code>ptp sync interval</code></td><td>Configures the interval between PTP synchronization messages on an interface.</td></tr> <tr> <td></td><td><code>ptp vlan vlan</code></td><td>Configures the PTP VLAN value on an interface.</td></tr> </tbody> </table> <p>Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 333.</p>	Related Commands	Command	Description		<code>ptp</code>	Enables or disables PTP on an interface.		<code>ptp announce</code>	Configures the interval between PTP announce messages on an interface or the number of PTP intervals before a timeout occurs on an interface.		<code>ptp sync interval</code>	Configures the interval between PTP synchronization messages on an interface.		<code>ptp vlan vlan</code>	Configures the PTP VLAN value on an interface.	<p>ptp announce interval</p> <p>The <code>ptp announce interval</code> command configures the interval between PTP announcement messages on or the number of PTP intervals before a timeout occurs. To disable this feature, use the <code>no</code> form of this command.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 315.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 253; Arista User Manual, v. 4.11.1 (1/11/13), at 199.</p>
Related Commands	Command	Description															
	<code>ptp</code>	Enables or disables PTP on an interface.															
	<code>ptp announce</code>	Configures the interval between PTP announce messages on an interface or the number of PTP intervals before a timeout occurs on an interface.															
	<code>ptp sync interval</code>	Configures the interval between PTP synchronization messages on an interface.															
	<code>ptp vlan vlan</code>	Configures the PTP VLAN value on an interface.															

Copyright Registration Information	Cisco	Arista															
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<p>ptp delay-request minimum interval</p> <p>To configure the minimum interval allowed between Precision Time Protocol (PTP) delay-request messages when the port is in the master state, use the ptp delay-request minimum interval command. To remove the minimum interval configuration for PTP delay-request messages, use the no form of this command.</p> <p>Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 332.</p>	<p>ptp delay-req interval</p> <p>The ptp delay-req interval command specifies the time recommended to the slave devices to send delay request messages. You must enable PTP on the switch first and configure the source IP address for PTP communication. To remove the minimum interval configuration for PTP delay-request messages, use the no form of this command.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 318.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 256; Arista User Manual, v. 4.11.1 (1/11/13), at 202.</p>															
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<table><tr><td>Related Commands</td><td>Command</td><td>Description</td></tr><tr><td></td><td>feature ptp</td><td>Enables or disables PTP on the device.</td></tr><tr><td></td><td>ptp source</td><td>Configures the source IP address for all PTP packets.</td></tr><tr><td></td><td>ptp priority1</td><td>Configures the priority1 value to use when advertising this clock.</td></tr><tr><td></td><td>ptp priority2</td><td>Configures the priority2 value to use when advertising this clock.</td></tr></table> <p>Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 334.</p>	Related Commands	Command	Description		feature ptp	Enables or disables PTP on the device.		ptp source	Configures the source IP address for all PTP packets.		ptp priority1	Configures the priority1 value to use when advertising this clock.		ptp priority2	Configures the priority2 value to use when advertising this clock.	<p>ptp source ip</p> <p>The ptp source ip command configures the source IP address for all PTP packets. The IP address can be in IPv4 format. To remove PTP settings, use the no form of this command.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 328.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 264; Arista User Manual, v. 4.11.1 (1/11/13), at 210.</p>
Related Commands	Command	Description															
	feature ptp	Enables or disables PTP on the device.															
	ptp source	Configures the source IP address for all PTP packets.															
	ptp priority1	Configures the priority1 value to use when advertising this clock.															
	ptp priority2	Configures the priority2 value to use when advertising this clock.															

Copyright Registration Information	Cisco	Arista																																	
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>ptp priority1</p> <p>To configure the priority1 value when advertising the Precision Time Protocol (PTP) clock, use the <code>ptp priority1</code> command. To remove the priority1 value, use the <code>no</code> form of this command.</p> <pre>ptp priority1 priority-number no ptp priority1 priority-number</pre> <table border="1"> <tr> <td>Syntax Description</td><td>priority-number</td><td>Priority number. The range is from 0 to 255.</td></tr> <tr> <td>Defaults</td><td colspan="2">255</td></tr> <tr> <td>Command Modes</td><td colspan="2">Global configuration mode (config)</td></tr> <tr> <td>Supported User Roles</td><td colspan="2">network-admin vdc-admin</td></tr> <tr> <td rowspan="2">Command History</td><td>Release</td><td>Modification</td></tr> <tr> <td>5.2(1)</td><td>This command was introduced.</td></tr> <tr> <td>Usage Guidelines</td><td colspan="2">This command does not require a license.</td></tr> <tr> <td rowspan="2">Examples</td><td colspan="2">This example shows how to configure the priority1 value when advertising the PTP clock:</td></tr> <tr> <td colspan="2"> <pre>switch# configure terminal switch(config)# ptp priority1 10</pre> </td></tr> <tr> <td rowspan="2"></td><td colspan="2">This example shows how to remove the priority1 value when advertising the PTP clock:</td></tr> <tr> <td colspan="2"> <pre>switch# configure terminal switch(config)# no ptp priority1 10</pre> </td></tr> <tr> <td></td><td colspan="2">Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 336.</td></tr> </table>	Syntax Description	priority-number	Priority number. The range is from 0 to 255.	Defaults	255		Command Modes	Global configuration mode (config)		Supported User Roles	network-admin vdc-admin		Command History	Release	Modification	5.2(1)	This command was introduced.	Usage Guidelines	This command does not require a license.		Examples	This example shows how to configure the priority1 value when advertising the PTP clock:		<pre>switch# configure terminal switch(config)# ptp priority1 10</pre>			This example shows how to remove the priority1 value when advertising the PTP clock:		<pre>switch# configure terminal switch(config)# no ptp priority1 10</pre>			Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 336.		<p>Set the PTP Priority1</p> <p>To configure the priority1 value when advertising the clock, use the <code>ptp priority1</code> command. This value overrides the default criteria for best master clock selection. Lower values take precedence.</p> <ul style="list-style-type: none"> The <code>ptp priority1</code> command configures the priority1 value of 120 to use when advertising the clock. <pre>switch(config)# ptp priority1 120 switch(config)#</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 272.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 214-15.</p>
Syntax Description	priority-number	Priority number. The range is from 0 to 255.																																	
Defaults	255																																		
Command Modes	Global configuration mode (config)																																		
Supported User Roles	network-admin vdc-admin																																		
Command History	Release	Modification																																	
	5.2(1)	This command was introduced.																																	
Usage Guidelines	This command does not require a license.																																		
Examples	This example shows how to configure the priority1 value when advertising the PTP clock:																																		
	<pre>switch# configure terminal switch(config)# ptp priority1 10</pre>																																		
	This example shows how to remove the priority1 value when advertising the PTP clock:																																		
	<pre>switch# configure terminal switch(config)# no ptp priority1 10</pre>																																		
	Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 336.																																		

Copyright Registration Information	Cisco	Arista																					
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<table border="1"> <tr> <th data-bbox="296 280 428 297">Related Commands</th><th data-bbox="449 280 554 297">Command</th><th data-bbox="642 280 722 297">Description</th></tr> <tr> <td></td><td><code>feature ptp</code></td><td>Enables or disables PTP on the device.</td></tr> <tr> <td></td><td><code>ptp source</code></td><td>Configures the source IP address for all PTP packets.</td></tr> <tr> <td></td><td><code>ptp domain</code></td><td>Configures the domain number to use for this clock.</td></tr> <tr> <td></td><td><code>ptp priority2</code></td><td>Configures the priority2 value to use when advertising this clock.</td></tr> <tr> <td></td><td><code>show ptp brief</code></td><td>Displays the PTP status.</td></tr> <tr> <td></td><td><code>show ptp clock</code></td><td>Displays the properties of the local clock.</td></tr> </table> <p>Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 336.</p>	Related Commands	Command	Description		<code>feature ptp</code>	Enables or disables PTP on the device.		<code>ptp source</code>	Configures the source IP address for all PTP packets.		<code>ptp domain</code>	Configures the domain number to use for this clock.		<code>ptp priority2</code>	Configures the priority2 value to use when advertising this clock.		<code>show ptp brief</code>	Displays the PTP status.		<code>show ptp clock</code>	Displays the properties of the local clock.	<p>ptp domain</p> <p>The <code>ptp domain</code> command configures the domain number to use for the clock. PTP domains allow you to use multiple independent PTP clocking subdomains on a single network. To remove PTP settings, use the <code>no</code> form of this command.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 319.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 257; Arista User Manual, v. 4.11.1 (1/11/13), at 204.</p>
Related Commands	Command	Description																					
	<code>feature ptp</code>	Enables or disables PTP on the device.																					
	<code>ptp source</code>	Configures the source IP address for all PTP packets.																					
	<code>ptp domain</code>	Configures the domain number to use for this clock.																					
	<code>ptp priority2</code>	Configures the priority2 value to use when advertising this clock.																					
	<code>show ptp brief</code>	Displays the PTP status.																					
	<code>show ptp clock</code>	Displays the properties of the local clock.																					

Copyright Registration Information	Cisco	Arista																				
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<p>ptp priority2</p> <p>To configure the priority2 value when advertising the Precision Time Protocol (PTP) clock, use the ptp priority2 command. To remove the priority2 value when advertising the PTP, use the no form of this command.</p> <pre>ptp priority2 priority-number no ptp priority2 priority-number</pre> <table><tr><td>Syntax Description</td><td><i>priority-number</i> Priority number. The range is from 0 to 255.</td></tr><tr><td>Defaults</td><td>255</td></tr><tr><td>Command Modes</td><td>Global configuration mode (config)</td></tr><tr><td>Supported User Roles</td><td>network-admin vdc-admin</td></tr><tr><td>Command History</td><td><table><tr><th>Release</th><th>Modification</th></tr><tr><td>5.2(1)</td><td>This command was introduced.</td></tr></table></td></tr><tr><td>Usage Guidelines</td><td>This command does not require a license.</td></tr><tr><td>Examples</td><td><p>This example shows how to configure the priority2 value when advertising the PTP clock:</p><pre>switch# configure terminal switch(config)# ptp priority2 1</pre><p>This example shows how to remove the priority2 value configuration for use when advertising the PTP clock:</p><pre>switch# configure terminal switch(config)# no ptp priority2 1</pre></td></tr><tr><td></td><td>Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 337.</td><td><p>Set the PTP Priority2</p><p>To configure the priority2 value when advertising this clock, use the ptp priority2 command. This value is used to decide between two devices that are otherwise equally matched in the default criteria.</p><ul style="list-style-type: none">The ptp priority2 command configures the priority2 value of 128 to use when advertising this clock.<pre>switch(config)# ptp priority2 128 switch(config)#</pre><p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 272.</p><p>See also Arista User Manual v. 4.12.3 (7/17/13), at 215.</p></td></tr></table>	Syntax Description	<i>priority-number</i> Priority number. The range is from 0 to 255.	Defaults	255	Command Modes	Global configuration mode (config)	Supported User Roles	network-admin vdc-admin	Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>5.2(1)</td><td>This command was introduced.</td></tr></table>	Release	Modification	5.2(1)	This command was introduced.	Usage Guidelines	This command does not require a license.	Examples	<p>This example shows how to configure the priority2 value when advertising the PTP clock:</p> <pre>switch# configure terminal switch(config)# ptp priority2 1</pre> <p>This example shows how to remove the priority2 value configuration for use when advertising the PTP clock:</p> <pre>switch# configure terminal switch(config)# no ptp priority2 1</pre>		Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 337.	<p>Set the PTP Priority2</p> <p>To configure the priority2 value when advertising this clock, use the ptp priority2 command. This value is used to decide between two devices that are otherwise equally matched in the default criteria.</p> <ul style="list-style-type: none">The ptp priority2 command configures the priority2 value of 128 to use when advertising this clock. <pre>switch(config)# ptp priority2 128 switch(config)#</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 272.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 215.</p>
	Syntax Description	<i>priority-number</i> Priority number. The range is from 0 to 255.																				
Defaults	255																					
Command Modes	Global configuration mode (config)																					
Supported User Roles	network-admin vdc-admin																					
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>5.2(1)</td><td>This command was introduced.</td></tr></table>	Release	Modification	5.2(1)	This command was introduced.																	
Release	Modification																					
5.2(1)	This command was introduced.																					
Usage Guidelines	This command does not require a license.																					
Examples	<p>This example shows how to configure the priority2 value when advertising the PTP clock:</p> <pre>switch# configure terminal switch(config)# ptp priority2 1</pre> <p>This example shows how to remove the priority2 value configuration for use when advertising the PTP clock:</p> <pre>switch# configure terminal switch(config)# no ptp priority2 1</pre>																					
	Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 337.	<p>Set the PTP Priority2</p> <p>To configure the priority2 value when advertising this clock, use the ptp priority2 command. This value is used to decide between two devices that are otherwise equally matched in the default criteria.</p> <ul style="list-style-type: none">The ptp priority2 command configures the priority2 value of 128 to use when advertising this clock. <pre>switch(config)# ptp priority2 128 switch(config)#</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 272.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 215.</p>																				

Copyright Registration Information	Cisco	Arista															
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<table><tr><th>Related Commands</th><th>Command</th><th>Description</th></tr><tr><td></td><td>feature ptp</td><td>Enables or disables PTP on the device.</td></tr><tr><td></td><td>ptp source</td><td>Configures the source IP address for all PTP packets.</td></tr><tr><td></td><td>ptp domain</td><td>Configures the domain number to use for this clock.</td></tr><tr><td></td><td>ptp priority1</td><td>Configures the priority1 value to use when advertising this clock.</td></tr></table> Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 337.	Related Commands	Command	Description		feature ptp	Enables or disables PTP on the device.		ptp source	Configures the source IP address for all PTP packets.		ptp domain	Configures the domain number to use for this clock.		ptp priority1	Configures the priority1 value to use when advertising this clock.	<p>ptp source ip</p> <p>The ptp source ip command configures the source IP address for all PTP packets. The IP address can be in IPv4 format. To remove PTP settings, use the no form of this command.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 10/2/2014), at 328.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 264; Arista User Manual, v. 4.11.1 (1/11/13), at 210.</p>
Related Commands	Command	Description															
	feature ptp	Enables or disables PTP on the device.															
	ptp source	Configures the source IP address for all PTP packets.															
	ptp domain	Configures the domain number to use for this clock.															
	ptp priority1	Configures the priority1 value to use when advertising this clock.															
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<table><tr><th>Related Commands</th><th>Command</th><th>Description</th></tr><tr><td></td><td>feature ptp</td><td>Enables or disables PTP on the device.</td></tr><tr><td></td><td>ptp source</td><td>Configures the source IP address for all PTP packets.</td></tr><tr><td></td><td>ptp domain</td><td>Configures the domain number to use for this clock.</td></tr><tr><td></td><td>ptp priority1</td><td>Configures the priority1 value to use when advertising this clock.</td></tr></table> Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 337.	Related Commands	Command	Description		feature ptp	Enables or disables PTP on the device.		ptp source	Configures the source IP address for all PTP packets.		ptp domain	Configures the domain number to use for this clock.		ptp priority1	Configures the priority1 value to use when advertising this clock.	<p>ptp domain</p> <p>The ptp domain command configures the domain number to use for the clock. PTP domains allow you to use multiple independent PTP clocking subdomains on a single network. To remove PTP settings, use the no form of this command.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 319.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 257; Arista User Manual, v. 4.11.1 (1/11/13), at 204.</p>
Related Commands	Command	Description															
	feature ptp	Enables or disables PTP on the device.															
	ptp source	Configures the source IP address for all PTP packets.															
	ptp domain	Configures the domain number to use for this clock.															
	ptp priority1	Configures the priority1 value to use when advertising this clock.															
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<table><tr><th>Command</th><th>Description</th></tr><tr><td>ptp priority1</td><td>Configures the priority1 value to use when advertising this clock.</td></tr><tr><td>ptp priority2</td><td>Configures the priority2 value to use when advertising this clock.</td></tr><tr><td>show ptp brief</td><td>Displays the PTP status.</td></tr><tr><td>show ptp clock</td><td>Displays the properties of the local clock.</td></tr></table> Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 340.	Command	Description	ptp priority1	Configures the priority1 value to use when advertising this clock.	ptp priority2	Configures the priority2 value to use when advertising this clock.	show ptp brief	Displays the PTP status.	show ptp clock	Displays the properties of the local clock.	<p>Set the PTP Priority1</p> <p>To configure the priority1 value when advertising the clock, use the ptp priority1 command. This value overrides the default criteria for best master clock selection. Lower values take precedence.</p> <ul style="list-style-type: none">The ptp priority1 command configures the priority1 value of 120 to use when advertising the clock. <pre>switch(config)# ptp priority1 120 switch(config)#</pre> <p>Set the PTP Priority2</p> <p>To configure the priority2 value when advertising this clock, use the ptp priority2 command. This value is used to decide between two devices that are otherwise equally matched in the default criteria.</p> <ul style="list-style-type: none">The ptp priority2 command configures the priority2 value of 128 to use when advertising this clock. <pre>switch(config)# ptp priority2 128 switch(config)#</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 272.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 214-15.</p>					
Command	Description																
ptp priority1	Configures the priority1 value to use when advertising this clock.																
ptp priority2	Configures the priority2 value to use when advertising this clock.																
show ptp brief	Displays the PTP status.																
show ptp clock	Displays the properties of the local clock.																

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>ptp sync interval</p> <p>To configure the interval between Precision Time Protocol (PTP) synchronization messages on an interface, use the <code>ptp sync interval</code> command. To remove the interval configuration for PTP messages synchronization, use the <code>no</code> form of this command.</p> <pre>ptp sync interval seconds no ptp sync interval seconds</pre> <p>Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 340.</p>	<p>Set the Peer Delay Request Interval</p> <p>To configure the minimum interval allowed between Precision Time Protocol (PTP) peer delay-request messages, use the <code>ptp pdelay-req interval</code> command.</p> <ul style="list-style-type: none"> The <code>ptp pdelay-req interval</code> command configures the minimum interval allowed between Precision Time Protocol (PTP) peer delay-request messages to 3. <pre>switch(config-if-Et5)# ptp pdelay-request interval 3 switch(config-if-Et5)#</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 273.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 216.</p>
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>ptp sync interval</p> <p>To configure the interval between Precision Time Protocol (PTP) synchronization messages on an interface, use the <code>ptp sync interval</code> command. To remove the interval configuration for PTP messages synchronization, use the <code>no</code> form of this command.</p> <pre>ptp sync interval seconds no ptp sync interval seconds</pre> <p>Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 340.</p>	<p>ptp delay-req interval</p> <p>The <code>ptp delay-req interval</code> command specifies the time recommended to the slave devices to send delay request messages. You must enable PTP on the switch first and configure the source IP address for PTP communication. To remove the minimum interval configuration for PTP delay-request messages, use the <code>no</code> form of this command.</p> <p>Platform Arad, FM6000 Command Mode Interface-Ethernet Configuration Interface-Port Channel Configuration</p> <p>Command Syntax</p> <pre>ptp delay-req interval log_interval no ptp delay-req interval default ptp delay-req interval</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 318.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 256; Arista User Manual, v. 4.11.1 (1/11/13), at 202.</p>

Copyright Registration Information	Cisco	Arista															
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<table border="1"> <thead> <tr> <th>Related Commands</th><th>Command</th><th>Description</th></tr> </thead> <tbody> <tr> <td></td><td><code>ptp</code></td><td>Enables or disables PTP on an interface.</td></tr> <tr> <td></td><td><code>ptp announce</code></td><td>Configures the interval between PTP announce messages on an interface or the number of PTP intervals before a timeout occurs on an interface.</td></tr> <tr> <td></td><td><code>ptp delay-request minimum interval</code></td><td>Configures the minimum interval allowed between PTP delay-request messages when the port is in the master state.</td></tr> <tr> <td></td><td><code>ptp vlan vlan</code></td><td>Configures the PTP VLAN value on an interface.</td></tr> </tbody> </table> <p>Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 342.</p>	Related Commands	Command	Description		<code>ptp</code>	Enables or disables PTP on an interface.		<code>ptp announce</code>	Configures the interval between PTP announce messages on an interface or the number of PTP intervals before a timeout occurs on an interface.		<code>ptp delay-request minimum interval</code>	Configures the minimum interval allowed between PTP delay-request messages when the port is in the master state.		<code>ptp vlan vlan</code>	Configures the PTP VLAN value on an interface.	<p>Examples</p> <ul style="list-style-type: none"> This command shows how to configure the minimum interval allowed between PTP delay-request messages. <pre>switch(config)# interface ethernet 5 switch(config-if-Et5)# ptp delay-request interval 3 switch(config-if-Et5)#</pre> This command removes the configured minimum interval allowed between PTP delay-request messages. <pre>switch(config)# interface ethernet 5 switch(config-if-Et5)# no ptp delay-request interval switch(config-if-Et5)#</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 318.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 256; Arista User Manual, v. 4.11.1 (1/11/13), at 202.</p>
Related Commands	Command	Description															
	<code>ptp</code>	Enables or disables PTP on an interface.															
	<code>ptp announce</code>	Configures the interval between PTP announce messages on an interface or the number of PTP intervals before a timeout occurs on an interface.															
	<code>ptp delay-request minimum interval</code>	Configures the minimum interval allowed between PTP delay-request messages when the port is in the master state.															
	<code>ptp vlan vlan</code>	Configures the PTP VLAN value on an interface.															
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>Make sure that you have globally enabled PTP on the device and configured the source IP address for PTP communication.</p> <p>Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 343.</p>	<p>The <code>ptp delay-req interval</code> command specifies the time recommended to the slave devices to send delay request messages. You must enable PTP on the switch first and configure the source IP address for PTP communication. To remove the minimum interval configuration for PTP delay-request messages, use the no form of this command.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 318.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 256; Arista User Manual, v. 4.11.1 (1/11/13), at 202.</p>															

Copyright Registration Information	Cisco	Arista															
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<table border="1"> <thead> <tr> <th>Related Commands</th><th>Command</th><th>Description</th></tr> </thead> <tbody> <tr> <td></td><td>ptp</td><td>Enables or disables PTP on an interface.</td></tr> <tr> <td></td><td>ptp announce</td><td>Configures the interval between PTP announce messages on an interface or the number of PTP intervals before a timeout occurs on an interface.</td></tr> <tr> <td></td><td>ptp delay-request minimum interval</td><td>Configures the minimum interval allowed between PTP delay-request messages when the port is in the master state.</td></tr> <tr> <td></td><td>ptp sync interval</td><td>Configures the interval between PTP synchronization messages on an interface.</td></tr> </tbody> </table> <p>Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 344.</p>	Related Commands	Command	Description		ptp	Enables or disables PTP on an interface.		ptp announce	Configures the interval between PTP announce messages on an interface or the number of PTP intervals before a timeout occurs on an interface.		ptp delay-request minimum interval	Configures the minimum interval allowed between PTP delay-request messages when the port is in the master state.		ptp sync interval	Configures the interval between PTP synchronization messages on an interface.	<p>ptp announce interval</p> <p>The ptp announce interval command configures the interval between PTP announcement messages on or the number of PTP intervals before a timeout occurs. To disable this feature, use the no form of this command.</p> <p>Platform Arad, FM6000 Command Mode Interface-Ethernet Configuration Interface-Port Channel Configuration</p> <p>Command Syntax</p> <pre>ptp announce interval log_interval no ptp announce interval default ptp announce interval</pre> <p>Parameters</p> <ul style="list-style-type: none"> <i>log_interval</i> The number of log seconds between PTP announcement message (base 2 log (seconds)). Value ranges from 0 to 4; default value is 1. <p>Examples</p> <ul style="list-style-type: none"> This command shows how to configure the interval between PTP announce messages on an interface. <pre>switch(config)# interface ethernet 5 switch(config-if-Et5)# ptp announce interval 1 switch(config-if-Et5)#</pre> This command removes the configured interval between PTP announce messages on interface Ethernet 5. <pre>switch(config)# interface ethernet 5 switch(config-if-Et5)# no ptp announce interval switch(config-if-Et5)#</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 315.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 253; Arista User Manual, v. 4.11.1 (1/11/13), at 199.</p>
Related Commands	Command	Description															
	ptp	Enables or disables PTP on an interface.															
	ptp announce	Configures the interval between PTP announce messages on an interface or the number of PTP intervals before a timeout occurs on an interface.															
	ptp delay-request minimum interval	Configures the minimum interval allowed between PTP delay-request messages when the port is in the master state.															
	ptp sync interval	Configures the interval between PTP synchronization messages on an interface.															

Copyright Registration Information	Cisco	Arista																														
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>snmp-server user</p> <p>To configure the Simple Network Management Protocol (SNMP) user information, use the snmp-server user command. To disable the configuration or to revert to factory defaults, use the no form of this command.</p> <pre>snmp-server user username [group-name] [auth {md5 sha} password [priv {aes-128} password] [localizedkey] [engineID id]] no snmp-server user username [group-name] [auth {md5 sha} password [priv {aes-128} password] [localizedkey] [engineID id]]</pre> <table border="1"> <tr> <td>Syntax Description</td><td>username</td><td>Name of the user. The name can be any case-sensitive, alphanumeric string up to 32 characters.</td></tr> <tr> <td></td><td>group-name</td><td>(Optional) Name of the group. The name can be any case-sensitive, alphanumeric string up to 32 characters.</td></tr> <tr> <td></td><td>auth</td><td>(Optional) Sets authentication parameters for the user.</td></tr> <tr> <td></td><td>md5</td><td>Uses the MD5 algorithm for authentication.</td></tr> <tr> <td></td><td>sha</td><td>Uses the SHA algorithm for authentication.</td></tr> <tr> <td></td><td>password</td><td>User password. The password can be any case-sensitive, alphanumeric string up to 64 characters. If you configure the localizedkey keyword, the password can be any case-sensitive, alphanumeric string up to 130 characters.</td></tr> <tr> <td></td><td>priv</td><td>(Optional) Sets encryption parameters for the user.</td></tr> <tr> <td></td><td>aes-128</td><td>(Optional) Sets the 128-byte AES algorithm for privacy.</td></tr> <tr> <td></td><td>localizedkey</td><td>(Optional) Sets passwords in the localized key format. If you configure this keyword, the password can be any case-sensitive, alphanumeric string up to 130 characters.</td></tr> <tr> <td></td><td>engineID id</td><td>(Optional) Configures the SNMP Engine ID for a notification target user. The engineID format is a 12-digit colon-separated decimal number.</td></tr> </table> <p>Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 394.</p>	Syntax Description	username	Name of the user. The name can be any case-sensitive, alphanumeric string up to 32 characters.		group-name	(Optional) Name of the group. The name can be any case-sensitive, alphanumeric string up to 32 characters.		auth	(Optional) Sets authentication parameters for the user.		md5	Uses the MD5 algorithm for authentication.		sha	Uses the SHA algorithm for authentication.		password	User password. The password can be any case-sensitive, alphanumeric string up to 64 characters. If you configure the localizedkey keyword, the password can be any case-sensitive, alphanumeric string up to 130 characters.		priv	(Optional) Sets encryption parameters for the user.		aes-128	(Optional) Sets the 128-byte AES algorithm for privacy.		localizedkey	(Optional) Sets passwords in the localized key format. If you configure this keyword, the password can be any case-sensitive, alphanumeric string up to 130 characters.		engineID id	(Optional) Configures the SNMP Engine ID for a notification target user. The engineID format is a 12-digit colon-separated decimal number.	<p>snmp-server user</p> <p>The snmp-server user command adds a user to a Simple Network Management Protocol (SNMP) group or modifies an existing user's parameters.</p> <p>To configure a remote user, specify the IP address or port number of the device where the user's remote SNMP agent resides. A remote agent's engine ID must be configured before remote users for that agent are configured. A user's authentication and privacy digests are derived from the engine ID and the user's password. The configuration command fails if the remote engine ID is not configured first.</p> <p>The no snmp-server user and default snmp-server user commands remove the user from an SNMP group by deleting the user command from <i>running-config</i>.</p> <p>Platform all Command Mode Global Configuration</p> <p>Command Syntax</p> <pre>snmp-server user user_name group_name [AGENT] VERSION [ENGINE] [SECURITY] no snmp-server user user_name group_name [AGENT] VERSION default snmp-server user user_name group_name [AGENT] VERSION</pre> <p>Parameters</p> <ul style="list-style-type: none"> user_name name of the user on the host that connects to the agent. group_name name of the group to which the user is associated. AGENT location of the host connecting to the SNMP agent. Configuration options include: <ul style="list-style-type: none"> <no parameter> local SNMP agent. remote addr [udp-port p_num] remote SNMP agent location (IP address, udp port). <i>addr</i> denotes the IP address; <i>p_num</i> denotes the udp port socket. (default port is 162). VERSION SNMP version; options include: <ul style="list-style-type: none"> v1 SNMPv1. v2c SNMPv2c. v3 SNMPv3; enables user-name match authentication. ENGINE engine ID used to localize passwords. Available only if VERSION is v3. <ul style="list-style-type: none"> <no parameter> Passwords localized by SNMP copy specified by <i>agent</i>. localized engineID octet string of engineID. SECURITY Specifies authentication and encryption levels. Available only if VERSION is v3. Encryption is available only when authentication is configured. <ul style="list-style-type: none"> <no parameter> no authentication or encryption. auth a_meth a_pass [priv e_meth e_pass] authentication and encryption parameters. <ul style="list-style-type: none"> <i>a_meth</i> authentication method: options are md5 (HMAC-MD5-96) and sha (HMAC-SHA-96). <i>a_pass</i> authentication string for users receiving packets. <i>e_meth</i> encryption method: tions are aes (AES-128) and des (CBC-DES). <i>e_pass</i> encryption string for the users sending packets. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1999.</p>
Syntax Description	username	Name of the user. The name can be any case-sensitive, alphanumeric string up to 32 characters.																														
	group-name	(Optional) Name of the group. The name can be any case-sensitive, alphanumeric string up to 32 characters.																														
	auth	(Optional) Sets authentication parameters for the user.																														
	md5	Uses the MD5 algorithm for authentication.																														
	sha	Uses the SHA algorithm for authentication.																														
	password	User password. The password can be any case-sensitive, alphanumeric string up to 64 characters. If you configure the localizedkey keyword, the password can be any case-sensitive, alphanumeric string up to 130 characters.																														
	priv	(Optional) Sets encryption parameters for the user.																														
	aes-128	(Optional) Sets the 128-byte AES algorithm for privacy.																														
	localizedkey	(Optional) Sets passwords in the localized key format. If you configure this keyword, the password can be any case-sensitive, alphanumeric string up to 130 characters.																														
	engineID id	(Optional) Configures the SNMP Engine ID for a notification target user. The engineID format is a 12-digit colon-separated decimal number.																														

Copyright Registration Information	Cisco	Arista
		<p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1689; Arista User Manual, v. 4.11.1 (1/11/13), at 1374; Arista User Manual v. 4.10.3 (10/22/12), at 1141; Arista User Manual v. 4.9.3.2 (5/3/12), at 896; Arista User Manual v. 4.8.2 (11/18/11), at 703; Arista User Manual v. 4.7.3 (7/18/11), at 559.</p>
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>Examples</p> <p>This example shows how to display the EEE status on an interface:</p> <pre>switch# show interface ethernet2/6 Ethernet2/6 is down (Link not connected) admin state is up, Dedicated Interface Hardware: 10000 Ethernet, address: 0022.5579.de41 (bia 001b.54c1.af5d) MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec reliability 255/255, txload 1/255, rxload 1/255 Encapsulation ARPA, medium is broadcast auto-duplex, auto-speed, media type is 10G Beacon is turned off Auto-Negotiation is turned off Input flow-control is off, output flow-control is off Auto-mdix is turned off Rate mode is shared Switchport monitor is off EtherType is 0x8100 EEE (efficient-ethernet) : n/a Last link flapped never Last clearing of "show interface" counters never 0 interface resets 30 seconds input rate 0 bits/sec, 0 packets/sec 30 seconds output rate 0 bits/sec, 0 packets/sec Load-Interval #2: 5 minute (300 seconds)</pre> <p>Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 514.</p>	<p>Example</p> <ul style="list-style-type: none"> This command assigns the MAC address of 001c.2804.17e1 to Ethernet interface 7, then displays interface parameters, including the assigned address. <pre>switch(config)#interface ethernet 7 switch(config-if-Et7)#mac-address 001c.2804.17e1 switch(config-if-Et7)#show interface ethernet 7 Ethernet3 is up, line protocol is up (connected) Hardware is Ethernet, address is 001c.2804.17e1 (bia 001c.7312.02e2) Description: b.e45 MTU 9212 bytes, BW 10000000 Kbit Full-duplex, 10Gb/s, auto negotiation: off Last clearing of "show interface" counters never 5 seconds input rate 7.84 kbps (0.0% with framing), 10 packets/sec 5 seconds output rate 270 kbps (0.0% with framing), 24 packets/sec 1363799 packets input, 222736140 bytes Received 0 broadcasts, 290904 multicast 0 runts, 0 giants 0 input errors, 0 CRC, 0 alignment, 0 symbol 0 PAUSE input 2264927 packets output, 2348747214 bytes Sent 0 broadcasts, 28573 multicast 0 output errors, 0 collisions 0 late collision, 0 deferred 0 PAUSE output switch(config-if-Et7)#</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 437.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 371; Arista User Manual, v. 4.11.1 (1/11/13), at 312; Arista User Manual v. 4.10.3 (10/22/12), at 270; Arista User Manual v. 4.9.3.2 (5/3/12), at 252.</p>

Copyright Registration Information	Cisco	Arista															
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<table border="1"> <tr> <th>Related Commands</th><th>Command</th><th>Description</th></tr> <tr> <td></td><td>show lldp tlv-select</td><td>Displays the LLDP TLV configuration.</td></tr> <tr> <td></td><td>lldp tlv-select</td><td>Specifies the TLVs to send and receive in LLDP packets.</td></tr> </table> <p>Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 515.</p>	Related Commands	Command	Description		show lldp tlv-select	Displays the LLDP TLV configuration.		lldp tlv-select	Specifies the TLVs to send and receive in LLDP packets.	<p>lldp tlv-select</p> <p>The <code>lldp tlv-select</code> command allows the user to specify the TLVs to send and receive in LLDP packets. The available TLVs are management-address, port-description, port-vlan, system-capabilities, system-description, and system-name.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 592.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 465; Arista User Manual, v. 4.11.1 (1/11/13), at 383.</p>						
Related Commands	Command	Description															
	show lldp tlv-select	Displays the LLDP TLV configuration.															
	lldp tlv-select	Specifies the TLVs to send and receive in LLDP packets.															
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<table border="1"> <tr> <th>Related Commands</th><th>Command</th><th>Description</th></tr> <tr> <td></td><td>show lldp traffic interface ethernet</td><td>Displays the number of LLDP packets sent and received on the interface.</td></tr> <tr> <td></td><td>show running-config lldp</td><td>Displays the global LLDP configuration.</td></tr> <tr> <td></td><td>lldp transmit</td><td>Enables the transmission of LLDP packets on an interface.</td></tr> <tr> <td></td><td>lldp receive</td><td>Enables the reception of LLDP packets on an interface.</td></tr> </table> <p>Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 522.</p>	Related Commands	Command	Description		show lldp traffic interface ethernet	Displays the number of LLDP packets sent and received on the interface.		show running-config lldp	Displays the global LLDP configuration.		lldp transmit	Enables the transmission of LLDP packets on an interface.		lldp receive	Enables the reception of LLDP packets on an interface.	<p>lldp transmit</p> <p>The <code>lldp transmit</code> command enables the transmission of LLDP packets on an interface. After you globally enable LLDP, it is enabled on all supported interfaces by default.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 593.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 466; Arista User Manual, v. 4.11.1 (1/11/13), at 384.</p>
Related Commands	Command	Description															
	show lldp traffic interface ethernet	Displays the number of LLDP packets sent and received on the interface.															
	show running-config lldp	Displays the global LLDP configuration.															
	lldp transmit	Enables the transmission of LLDP packets on an interface.															
	lldp receive	Enables the reception of LLDP packets on an interface.															
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<table border="1"> <tr> <th>Related Commands</th><th>Command</th><th>Description</th></tr> <tr> <td></td><td>show lldp holdtime</td><td>Specifies the amount of time in seconds that a receiving device should hold the information sent by your device before discarding it.</td></tr> <tr> <td></td><td>lldp reinit</td><td>Specifies the delay time in seconds for LLDP to initialize on any interface.</td></tr> <tr> <td></td><td>lldp timer</td><td>Specifies the transmission frequency of LLDP updates in seconds.</td></tr> </table> <p>Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 522.</p>	Related Commands	Command	Description		show lldp holdtime	Specifies the amount of time in seconds that a receiving device should hold the information sent by your device before discarding it.		lldp reinit	Specifies the delay time in seconds for LLDP to initialize on any interface.		lldp timer	Specifies the transmission frequency of LLDP updates in seconds.	<p>12.3.3.2 Setting the LLDP Hold Time</p> <p>The <code>lldp holdtime</code> command specifies the amount of time in seconds that a receiving device should hold the information sent by the device before discarding it.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 578.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 450; Arista User Manual, v. 4.11.1 (1/11/13), at 368</p>			
Related Commands	Command	Description															
	show lldp holdtime	Specifies the amount of time in seconds that a receiving device should hold the information sent by your device before discarding it.															
	lldp reinit	Specifies the delay time in seconds for LLDP to initialize on any interface.															
	lldp timer	Specifies the transmission frequency of LLDP updates in seconds.															

Copyright Registration Information	Cisco	Arista												
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<table border="1"> <thead> <tr> <th>Related Commands</th><th>Command</th><th>Description</th></tr> </thead> <tbody> <tr> <td></td><td>show lldp holdtime</td><td>Specifies the amount of time in seconds that a receiving device should hold the information sent by your device before discarding it.</td></tr> <tr> <td></td><td>lldp reinit</td><td>Specifies the delay time in seconds for LLDP to initialize on any interface.</td></tr> <tr> <td></td><td>lldp timer</td><td>Specifies the transmission frequency of LLDP updates in seconds.</td></tr> </tbody> </table> <p>Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 522.</p>	Related Commands	Command	Description		show lldp holdtime	Specifies the amount of time in seconds that a receiving device should hold the information sent by your device before discarding it.		lldp reinit	Specifies the delay time in seconds for LLDP to initialize on any interface.		lldp timer	Specifies the transmission frequency of LLDP updates in seconds.	<p>lldp reinit</p> <p>The lldp reinit command specifies the delay time in seconds for LLDP to initialize on any interface.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 589.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 462; Arista User Manual, v. 4.11.1 (1/11/13), at 380.</p>
Related Commands	Command	Description												
	show lldp holdtime	Specifies the amount of time in seconds that a receiving device should hold the information sent by your device before discarding it.												
	lldp reinit	Specifies the delay time in seconds for LLDP to initialize on any interface.												
	lldp timer	Specifies the transmission frequency of LLDP updates in seconds.												
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<table border="1"> <thead> <tr> <th>Related Commands</th><th>Command</th><th>Description</th></tr> </thead> <tbody> <tr> <td></td><td>show lldp traffic interface ethernet</td><td>Displays the number of LLDP packets sent and received on the interface.</td></tr> <tr> <td></td><td>show running-config lldp</td><td>Displays the global LLDP configuration.</td></tr> </tbody> </table> <p>Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 527.</p>	Related Commands	Command	Description		show lldp traffic interface ethernet	Displays the number of LLDP packets sent and received on the interface.		show running-config lldp	Displays the global LLDP configuration.	<p>show lldp traffic</p> <p>The show lldp traffic command displays LLDP counters, including the number of packets sent and received, and the number of packets discarded.</p> <p>Platform all Command Mode EXEC</p> <p>Command Syntax</p> <p>show lldp traffic [INTERFACE]</p> <p>Parameters</p> <ul style="list-style-type: none"> • INTERFACE Interface type and numbers. Options include: <ul style="list-style-type: none"> — <no parameter> Display information for all interfaces. — ethernet <i>e_range</i> Ethernet interface range specified by <i>e_range</i>. — management <i>m_range</i> Management interface range specified by <i>m_range</i>. <p>Valid <i>e_range</i> and <i>m_range</i> formats include number, number range, or comma-delimited list of numbers and ranges.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 599.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 472; Arista User Manual, v. 4.11.1 (1/11/13), at 390.</p>			
Related Commands	Command	Description												
	show lldp traffic interface ethernet	Displays the number of LLDP packets sent and received on the interface.												
	show running-config lldp	Displays the global LLDP configuration.												

Copyright Registration Information	Cisco	Arista									
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<table border="1"> <thead> <tr> <th>Related Commands</th><th>Command</th><th>Description</th></tr> </thead> <tbody> <tr> <td></td><td><code>show lldp traffic</code></td><td>Displays the LLDP counters, including the number of LLDP packets sent and received by the device, the number of discarded packets, and the number of unrecognized TLVs.</td></tr> <tr> <td></td><td><code>show running-config lldp</code></td><td>Displays the global LLDP configuration.</td></tr> </tbody> </table> <p>Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 529.</p>	Related Commands	Command	Description		<code>show lldp traffic</code>	Displays the LLDP counters, including the number of LLDP packets sent and received by the device, the number of discarded packets, and the number of unrecognized TLVs.		<code>show running-config lldp</code>	Displays the global LLDP configuration.	<p>show lldp traffic</p> <p>The <code>show lldp traffic</code> command displays LLDP counters, including the number of packets sent and received, and the number of packets discarded.</p> <p>Platform all Command Mode EXEC</p> <p>Command Syntax</p> <p><code>show lldp traffic [INTERFACE]</code></p> <p>Parameters</p> <ul style="list-style-type: none"> <i>INTERFACE</i> Interface type and numbers. Options include: <ul style="list-style-type: none"> <code><no parameter></code> Display information for all interfaces. <code>ethernet e_range</code> Ethernet interface range specified by <i>e_range</i>. <code>management m_range</code> Management interface range specified by <i>m_range</i>. <p>Valid <i>e_range</i> and <i>m_range</i> formats include number, number range, or comma-delimited list of numbers and ranges.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 599.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 472; Arista User Manual, v. 4.11.1 (1/11/13), at 390.</p>
Related Commands	Command	Description									
	<code>show lldp traffic</code>	Displays the LLDP counters, including the number of LLDP packets sent and received by the device, the number of discarded packets, and the number of unrecognized TLVs.									
	<code>show running-config lldp</code>	Displays the global LLDP configuration.									

Copyright Registration Information	Cisco	Arista				
<div>Cisco NX-OS 6.2</div> <div>Effective date of registration: 11/13/2014</div>	<div><div>show ptp clock</div><div>To display the Precision Time Protocol (PTP) clock information, use the show ptp clock command.</div><div>show ptp clock</div><div><div>Syntax Description</div><div>This command has no arguments or keywords.</div></div><div><div>Defaults</div><div>None</div></div><div><div>Command Modes</div><div>Any command mode</div></div><div><div>Supported User Roles</div><div>network-admin network-operator vdc-admin vdc-operator</div></div><div><div>Command History</div><table><tr><th>Release</th><th>Modification</th></tr><tr><td>5.2(1)</td><td>This command was introduced.</td></tr></table></div><div><div>Usage Guidelines</div><div>This command does not require a license.</div></div><div><div>Examples</div><div>This example shows how to display the PTP clock information:</div><div>switch# show ptp clock ptp device type: boundary clock Clock Identity: 0:18:ba:ff:ff:d8:0:17 Clock Domain: 0 Number of PTP ports: 2 Priority1: 255 Priority2: 255 Clock Quality: Class: 48 Accuracy: 254 Offset (log variance): 65535 Offset From Master: 0 Mean Path Delay: 0 Steps removed: 1 Local clock time: Sun Jan 15 20:57:29 2013</div></div></div>	Release	Modification	5.2(1)	This command was introduced.	<div><div>Show PTP Clock and Offset</div><div>To display the Precision Time Protocol (PTP) local clock and offset, use the show ptp clock command.</div><div><ul style="list-style-type: none">The show ptp clock command displays the Precision Time Protocol (PTP) local clock and offset.</div><div>switch# show ptp clock PTP Mode: Boundary Clock Clock Identity: 0x00:1e:73:ff:ff:1a:83:24 Clock Domain: 1 Number of PTP ports: 24 Priority1: 128 Priority2: 128 Clock Quality: Class: 248 Accuracy: 0x30 Offset Scaled Log Variance: 0xffff Offset From Master: 0 Mean Path Delay: 0 Steps Removed: 0 switch#</div><div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 275.</div><div>See also Arista User Manual v. 4.12.3 (7/17/13), at 217.</div></div>
	Release	Modification				
5.2(1)	This command was introduced.					

Copyright Registration Information	Cisco	Arista																																												
<div>Cisco NX-OS 6.2</div> <div>Effective date of registration: 11/13/2014</div>	<div><div>show ptp clock foreign-masters-record</div><div>To display information about the state of foreign masters known to the Precision Time Protocol (PTP) process, use the show ptp clocks foreign-masters-record command.</div><div>show ptp clock foreign-masters-record {interface [ethernet]}</div><div><table><tr><td>Syntax Description</td><td>interface</td><td>Specifies an interface.</td></tr><tr><td></td><td>ethernet</td><td>(Optional) Specifies an Ethernet interface.</td></tr></table></div><div><table><tr><td>Defaults</td><td>None</td></tr></table></div><div><table><tr><td>Command Modes</td><td>Any command mode</td></tr></table></div><div><table><tr><td>Supported User Roles</td><td>network-admin network-operator vdc-admin vdc-operator</td></tr></table></div><div><table><tr><td>Command History</td><td><table><tr><th>Release</th><th>Modification</th></tr><tr><td>5.2(1)</td><td>This command was introduced.</td></tr></table></td></tr></table></div><div><table><tr><td>Usage Guidelines</td><td>This command does not require a license.</td></tr></table></div><div><div><div>Examples</div><div>This example shows how to display information about the state of foreign masters known to the PTP process:</div><div>switch# show ptp clock foreign-masters-record interface ethernet 7/1 EP/0/0/CP00.demo#show ptp clocks foreign-masters P1=Priority1, P2=Priority2, C=Class, A=Accuracy, OSLV=offset-scaled-log-variance, SR=steps-removed CM=is grandmaster</div><div><table><tr><th>Interface</th><th>Clock-ID</th><th>P1</th><th>P2</th><th>C</th><th>A</th><th>OSLV</th><th>SR</th></tr><tr><td>Eth7/10</td><td>0:18:ba:ff:ff:d8: e:16</td><td>255</td><td>255</td><td>240</td><td>254</td><td>65535</td><td>0 GM</td></tr><tr><td>Eth7/1</td><td>0:18:ba:ff:ff:d8: e:16</td><td>255</td><td>255</td><td>240</td><td>254</td><td>65535</td><td>0 GM</td></tr></table></div></div></div></div>	Syntax Description	interface	Specifies an interface.		ethernet	(Optional) Specifies an Ethernet interface.	Defaults	None	Command Modes	Any command mode	Supported User Roles	network-admin network-operator vdc-admin vdc-operator	Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>5.2(1)</td><td>This command was introduced.</td></tr></table>	Release	Modification	5.2(1)	This command was introduced.	Usage Guidelines	This command does not require a license.	Interface	Clock-ID	P1	P2	C	A	OSLV	SR	Eth7/10	0:18:ba:ff:ff:d8: e:16	255	255	240	254	65535	0 GM	Eth7/1	0:18:ba:ff:ff:d8: e:16	255	255	240	254	65535	0 GM	<div><div>Show PTP Foreign Master</div><div>To display information about the state of foreign masters known to the Precision Time Protocol (PTP) process, use the show ptp foreign-master-record command.</div><div><ul style="list-style-type: none">The show ptp foreign-master-records command displays information about the state of foreign masters known to the PTP process.</div><div><div>switch# show ptp clocks foreign-masters-record</div><div>No Foreign Master Records</div><div>switch#</div></div><div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 277.</div><div>See also Arista User Manual v. 4.12.3 (7/17/13), at 219-220.</div></div>
	Syntax Description	interface	Specifies an interface.																																											
	ethernet	(Optional) Specifies an Ethernet interface.																																												
Defaults	None																																													
Command Modes	Any command mode																																													
Supported User Roles	network-admin network-operator vdc-admin vdc-operator																																													
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>5.2(1)</td><td>This command was introduced.</td></tr></table>	Release	Modification	5.2(1)	This command was introduced.																																									
Release	Modification																																													
5.2(1)	This command was introduced.																																													
Usage Guidelines	This command does not require a license.																																													
Interface	Clock-ID	P1	P2	C	A	OSLV	SR																																							
Eth7/10	0:18:ba:ff:ff:d8: e:16	255	255	240	254	65535	0 GM																																							
Eth7/1	0:18:ba:ff:ff:d8: e:16	255	255	240	254	65535	0 GM																																							

Copyright Registration Information	Cisco	Arista														
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<div>Examples</div> <div>This example shows how to display information about the state of foreign masters known to the PTP process:</div> <div>switch# show ptp clock foreign-masters-record interface ethernet 7/1 EP/0/0/CPUG:demo#show ptp clocks foreign-masters P1=Priority1, P2=Priority2, C=Class, A=Accuracy, OSLV=Offset-Scaled-Log-Variance, SR=Steps-Removed GM=is grandmaster</div> <table><thead><tr><th>Interface</th><th>Clock-ID</th><th>P1</th><th>P2</th><th>C</th><th>A</th><th>OSLV</th><th>SR</th></tr></thead><tbody><tr><td>Eth7/1/0</td><td>0.10:ba:ff:ff:d0: e:16 255 255 240 254 65535 0</td><td>GM</td></tr><tr><td>Eth7/1</td><td>0.10:ba:ff:ff:d0: e:16 255 255 240 254 65535 0</td><td>GM</td></tr></tbody></table> <div>Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 603.</div>	Interface	Clock-ID	P1	P2	C	A	OSLV	SR	Eth7/1/0	0.10:ba:ff:ff:d0: e:16 255 255 240 254 65535 0	GM	Eth7/1	0.10:ba:ff:ff:d0: e:16 255 255 240 254 65535 0	GM	<div>Examples</div> <div><ul style="list-style-type: none">This command shows how to display information about the state of foreign masters known to the PTP process.</div> <div>switch# show ptp clocks foreign-masters-record No Foreign Master Records switch#</div> <div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 349.</div> <div>See also Arista User Manual v. 4.12.3 (7/17/13), at 282; Arista User Manual, v. 4.11.1 (1/11/13), at 228.</div>
Interface	Clock-ID	P1	P2	C	A	OSLV	SR									
Eth7/1/0	0.10:ba:ff:ff:d0: e:16 255 255 240 254 65535 0	GM														
Eth7/1	0.10:ba:ff:ff:d0: e:16 255 255 240 254 65535 0	GM														

Copyright Registration Information	Cisco	Arista				
<div>Cisco NX-OS 6.2</div> <div>Effective date of registration: 11/13/2014</div>	<div><div>show ptp parent</div><div>To display information about the parent and grand master of the Precision Time Protocol (PTP) clock, use the show ptp parent command.</div><div>show ptp parent</div><div><div>Syntax Description</div><div>This command has no arguments or keywords.</div></div><div><div>Defaults</div><div>None</div></div><div><div>Command Modes</div><div>Any command mode</div></div><div><div>Supported User Roles</div><div>network-admin network-operator vdc-admin vdc-operator</div></div><div><div>Command History</div><div><table><tr><th>Release</th><th>Modification</th></tr><tr><td>5.2(1)</td><td>This command was introduced.</td></tr></table></div></div><div><div>Usage Guidelines</div><div>This command does not require a license.</div></div><div><div>Examples</div><div><div>This example shows how to display information about the parent and grand master of the PTP clock:</div><div>switch# show ptp parent Parent Clock: Parent Clock Identity: 0:18:ba:ff:ff:d8: a:16 Parent Port Number: 1546 Observed Parent Offset (log variance): N/A Observed Parent Clock Phase Change Rate: N/A Grandmaster Clock: Grandmaster Clock Identity: 0:18:ba:ff:ff:d8: a:16 Grandmaster Clock Quality: Class: 248 Accuracy: 254 Offset (log variance): 65535 Priority1: 255 Priority2: 255</div></div></div></div>	Release	Modification	5.2(1)	This command was introduced.	<div><div>Show PTP Parent Information</div><div>To display information about the parent and grand master of the Precision Time Protocol (PTP) clock, use the show ptp parent command.</div><div><ul style="list-style-type: none">The show ptp parent command displays information about the parent and grand master of the Precision Time Protocol (PTP) clock.</div><div><div>switch# show ptp parent Parent Clock: Parent Clock Identity: 0x00:1c:73:ff:ff:00:72:40 Parent Port Number: 0 Parent IP Address: N/A Observed Parent Offset (log variance): N/A Observed Parent Clock Phase Change Rate: N/A Grandmaster Clock: Grandmaster Clock Identity: 0x00:1c:73:ff:ff:00:72:40 Grandmaster Clock Quality: Class: 248 Accuracy: 0x30 Offset Scaled Log Variance: 0xffff Priority1: 128 Priority2: 128 switch#</div></div></div>
	Release	Modification				
5.2(1)	This command was introduced.					
<div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 275.</div> <div>See also Arista User Manual v. 4.12.3 (7/17/13), at 217.</div>						

Copyright Registration Information	Cisco	Arista				
<div>Cisco NX-OS 6.2</div> <div>Effective date of registration: 11/13/2014</div>	<div><div>show ptp parent</div><div>To display information about the parent and grand master of the Precision Time Protocol (PTP) clock, use the show ptp parent command.</div><div>show ptp parent</div><div><div>Syntax Description</div><div>This command has no arguments or keywords.</div></div><div><div>Defaults</div><div>None</div></div><div><div>Command Modes</div><div>Any command mode</div></div><div><div>Supported User Roles</div><div>network-admin network-operator vdc-admin vdc-operator</div></div><div><div>Command History</div><table><tr><th>Release</th><th>Modification</th></tr><tr><td>5.2(1)</td><td>This command was introduced.</td></tr></table></div><div><div>Usage Guidelines</div><div>This command does not require a license.</div></div><div><div>Examples</div><div>This example shows how to display information about the parent and grand master of the PTP clock:</div><div>switch# show ptp parent Parent Clock: Parent Clock Identity: 0:10:0a:ff:ff:d8: a:16 Parent Port Number: 1546 Observed Parent Offset (log variance): N/A Observed Parent Clock Phase Change Rate: N/A Grandmaster Clock: Grandmaster Clock Identity: 0:10:0a:ff:ff:d8: a:16 Grandmaster Clock Quality: Class: 248 Accuracy: 254 Offset (log variance): 65535 Priority1: 255 Priority2: 255</div></div></div>	Release	Modification	5.2(1)	This command was introduced.	<div><div>show ptp parent</div><div>The show ptp parent command displays information about the parent and grand master of the Precision Time Protocol (PTP) clock.</div><div>Platform Arad, FM6000 Command Mode Privileged EXEC</div><div><div>Command Syntax</div><div>show ptp parent</div></div><div><div>Examples</div><div><ul style="list-style-type: none">This command shows how to display information about the parent and master of the PTP clock.<div>switch# show ptp parent Parent Clock: Parent Clock Identity: 0x00:1c:73:ff:ff:00:72:40 Parent Port Number: 0 Parent IP Address: N/A Observed Parent Offset (log variance): N/A Observed Parent Clock Phase Change Rate: N/A Grandmaster Clock: Grandmaster Clock Identity: 0x00:1c:73:ff:ff:00:72:40 Grandmaster Clock Quality: Class: 248 Accuracy: 0x30 Offset Scaled Log Variance: 0xffff Priority1: 128 Priority2: 128 switch#</div></div></div></div>
	Release	Modification				
5.2(1)	This command was introduced.					

Copyright Registration Information	Cisco	Arista				
<div>Cisco NX-OS 6.2</div> <div>Effective date of registration: 11/13/2014</div>	<div><div>show ptp time-property</div><div>To display the Precision Time Protocol (PTP) clock properties, use the show ptp time-property command.</div><div>show ptp time-property</div></div> <div><div>Syntax Description</div><div>This command has no arguments or keywords.</div></div> <div><div>Defaults</div><div>None</div></div> <div><div>Command Modes</div><div>Any command mode</div></div> <div><div>SupportedUserRoles</div><div>network-admin network-operator vdc-admin vdc-operator</div></div> <div><div>Command History</div><table><tr><th>Release</th><th>Modification</th></tr><tr><td>5.2(1)</td><td>This command was introduced.</td></tr></table></div> <div><div>Usage Guidelines</div><div>This command does not require a license.</div></div> <div><div>Examples</div><div>This example shows how to display the PTP clock properties:</div><div>switch# show ptp time-property PTP CLOCK TIME PROPERTY: Current UTC Offset valid: 0 Current UTC Offset: 33 Leap59: 0 Leap61: 0 Time Traceable: 0 Frequency Traceable: 0 PTP Timescale: 0 Time Source: 0x0 (Internal Oscillator)</div></div> <div>Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 611.</div>	Release	Modification	5.2(1)	This command was introduced.	<div><div>Show PTP Clock Properties</div><div>To display the Precision Time Protocol (PTP) clock properties, use the show ptp time-property command.</div><div><div>The show ptp time-property command displays the Precision Time Protocol (PTP) clock properties.</div><div>switch# show ptp time-property Current UTC offset valid: False Current UTC offset: 0 Leap 59: False Leap 61: False Time Traceable: False Frequency Traceable: False PTP Timescale: False Time Source: 0x0 switch#</div></div><div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 275-76.</div><div>See also Arista User Manual v. 4.12.3 (7/17/13), at 218.</div></div>
	Release	Modification				
5.2(1)	This command was introduced.					

Copyright Registration Information	Cisco	Arista				
<div>Cisco NX-OS 6.2</div> <div>Effective date of registration: 11/13/2014</div>	<div><div>show ptp time-property</div><div>To display the Precision Time Protocol (PTP) clock properties, use the show ptp time-property command.</div><div>show ptp time-property</div><div><div>Syntax Description</div><div>This command has no arguments or keywords.</div></div><div><div>Defaults</div><div>None</div></div><div><div>Command Modes</div><div>Any command mode</div></div><div><div>SupportedUserRoles</div><div>network-admin network-operator vde-admin vde-operator</div></div><div><div>Command History</div><table><tr><th>Release</th><th>Modification</th></tr><tr><td>5.2(1)</td><td>This command was introduced.</td></tr></table></div><div><div>Usage Guidelines</div><div>This command does not require a license.</div></div><div><div>Examples</div><div>This example shows how to display the PTP clock properties:</div><div>switch# show ptp time-property PTP CLOCK TIME PROPERTY: Current UTC Offset valid: 0 Current UTC Offset: 33 Leap59: 0 Leap61: 0 Time Traceable: 0 Frequency Traceable: 0 PTP Timescale: 0 Time Source: 0xA0 (Internal Oscillator)</div></div></div>	Release	Modification	5.2(1)	This command was introduced.	<div><div>show ptp time-property</div><div>The show ptp time-property command displays the Precision Time Protocol (PTP) clock properties.</div><div>PlatformArad, FM6000 Command ModePrivileged EXEC</div><div><div>Command Syntax</div><div>show ptp time-property</div></div><div><div>Examples</div><div><ul style="list-style-type: none">This command shows the PTP clock properties.<div>switch# show ptp time-property Current UTC offset valid: False Current UTC offset: 0 Leap 59: False Leap 61: False Time Traceable: False Frequency Traceable: False PTP Timescale: False Time Source: 0x0 switch#</div></div></div></div> <div><div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 354.</div><div>See also Arista User Manual v. 4.12.3 (7/17/13), at 287; Arista User Manual, v. 4.11.1 (1/11/13), at 233.</div></div>
	Release	Modification				
5.2(1)	This command was introduced.					

<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<div data-bbox="310 224 1136 706"><div data-bbox="310 224 415 256">Examples</div><div data-bbox="520 232 1100 256">This example shows how to display the SNMP information:</div><pre data-bbox="520 272 1136 706">switch(config)# show snmp sys contact: sys location: anyplace, Anywhere 0 SNMP packets input 0 Bad SNMP versions 0 Unknown community name 0 Illegal operation for community name supplied 0 Encoding errors 0 Number of requested variables 0 Number of altered variables 0 Get-request PDUs 0 Get-next PDUs 0 Set-request PDUs 0 SNMP packets output 0 Too big errors 0 No such name errors 0 Bad values errors 0 General errors</pre></div> <p data-bbox="300 760 1073 816">Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 634.</p>	<div data-bbox="1178 224 2028 906"><div data-bbox="1178 224 1276 248">Example</div><ul data-bbox="1178 248 2028 272" style="list-style-type: none">This command configures xyz-1234 as the chassis-ID string, then displays the result.<pre data-bbox="1255 280 1965 906">switch(config)#snmp-server chassis-id xyz-1234 switch(config)#show snmp Chassis: xyz-1234 <---chassis ID 8 SNMP packets input 0 Bad SNMP version errors 0 Unknown community name 0 Illegal operation for community name supplied 0 encoding errors 8 Number of requested variables 0 Number of altered variables 4 Get-request PDUs 4 Get-next PDUs 0 Set-request PDUs 21 SNMP packets output 0 Too big errors 0 No such name errors 0 Bad value errors 0 General errors 8 Response PDUs 0 Trap PDUs SNMP logging: enabled Logging to taccon.162 SNMP agent enabled switch(config)#</pre></div> <p data-bbox="1171 954 1871 979">Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 354.</p> <p data-bbox="1171 1019 2032 1182"><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1657-58; Arista User Manual, v. 4.11.1 (1/11/13), at 1344-45; Arista User Manual v. 4.10.3 (10/22/12), at 1111; Arista User Manual v. 4.9.3.2 (5/3/12), at 867; Arista User Manual v. 4.8.2 (11/18/11), at 678; Arista User Manual v. 4.7.3 (7/18/11), at 549.</p>
--	--	---

Cisco NX-OS 6.2

Effective date of
registration:
11/13/2014

show snmp engineID

To display the Simple Network Management Protocol (SNMP) engine ID, use the show snmp engineID command.

show snmp engineID

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the SNMP engine ID:

switch(config)# show snmp engineID
Local SNMP engineID: [Hex] 80000009030005300A0B0C
[Dec] 128:000:000:009:003:000:005:048:010:011:012

Related Commands

Command	Description
snmp-server user	Configures SNMP target notification users.

Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 639.

show snmp engineID

The show snmp engineID command displays the identification of the local Simple Network Management Protocol (SNMP) engine and of all remote engines that are configured on the switch.

Platform

all

Command Mode

EXEC

Command Syntax

show snmp engineID

Example

- This command displays the ID of the local SNMP engine.

switch>show snmp engineid
Local SNMP EngineID: f5717f001c730436d700
switch>

Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1978.

See also Arista User Manual v. 4.12.3 (7/17/13), at 1668; Arista User Manual, v. 4.11.1 (1/11/13), at 1355; Arista User Manual v. 4.10.3 (10/22/12), at 1122; Arista User Manual v. 4.9.3.2 (5/3/12), at 878; Arista User Manual v. 4.8.2 (11/18/11), at 686; Arista User Manual v. 4.7.3 (7/18/11), at 542.

<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>Precision Time Protocol</p> <p>The Precision Time Protocol (PTP) is a time synchronization protocol for nodes distributed across a network. Its hardware timestamp feature provides greater accuracy than other time synchronization protocols such as Network Time Protocol (NTP). For more information about PTP, see Chapter 4, "Configuring PTP."</p> <p>Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 1-3.</p>	<p>5.3.2 Precision Time Protocol (PTP)</p> <p>The Precision Time Protocol (PTP) can substantially enhance the accuracy of real-time clocks in networked devices by providing sub-microsecond clock synchronization. Inbound clock signals are organized into a master-slave hierarchy. PTP identifies the switch port that is connected to the device with the most precise clock. This clock is referred to as the master clock. All the other devices on the network synchronize their clocks with the master and are referred to as slaves.</p> <p>The master clock sends out a sync message every second. The slave clock sends a delay request message to the master clock noting the time it was sent in order to measure and eliminate packet delays. The master clock then replies with the time stamp the delay message was received. The slave clock then computes the master clock time compensated for delays and finalizes synchronization. Constantly exchanged timing messages ensure continued synchronization.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 270.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 213; Arista User Manual, v. 4.11.1 (1/11/13), at 163.</p>
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>SNMP</p> <p>The Simple Network Management Protocol (SNMP) is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language used for the monitoring and management of devices in a network. For more information, see Chapter 11, "Configuring SNMP."</p> <p>Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 1-5.</p>	<p>37.2 SNMP Conceptual Overview</p> <p>Simple Network Management Protocol (SNMP) is an application-layer protocol that provides a standardized framework and a common language to monitor and manage network devices.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1961.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1651; Arista User Manual, v. 4.11.1 (1/11/13), at 1338; Arista User Manual v. 4.10.3 (10/22/12), at 1105; Arista User Manual v. 4.9.3.2 (5/3/12), at 861; Arista User Manual v. 4.8.2 (11/18/11), at 673; Arista User Manual v. 4.7.3 (7/18/11), at 529.</p>
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>SNMP</p> <p>The Simple Network Management Protocol (SNMP) is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language used for the monitoring and management of devices in a network. For more information, see Chapter 11, "Configuring SNMP."</p> <p>Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 1-5.</p>	<p>Chapter 37 SNMP</p> <p>SNMP is an application-layer protocol that provides a standardized framework and a common language to monitor and manage network devices.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 43.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 37; Arista User Manual, v. 4.11.1 (1/11/13), at 31; Arista User Manual v. 4.10.3 (10/22/12), at 28; Arista User Manual v. 4.9.3.2 (5/3/12), at 24; Arista User Manual v. 4.8.2 (11/18/11), at 20; Arista User Manual v. 4.7.3 (7/18/11), at 18.</p>

Cisco NX-OS 6.2

Effective date of
registration:
11/13/2014**Configuring the NTP Source IP Address**

NTP sets the source IP address for all NTP packets based on the address of the interface through which the NTP packets are sent. You can configure NTP to use a specific source IP address.

To configure the NTP source IP address, use the following command in global configuration mode:

Command	Purpose
[no] ntp source <i>ip-address</i>	Configures the source IP address for all NTP packets. The <i>ip-address</i> can be in IPv4 or IPv6 format.
Example. switch(config)# ntp source 192.0.2.1	

Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 3-16.

Configure the Source IP

To configure the source IP address for all PTP packets, use the **ptp source ip** command.

- The **ptp source ip** command configures the source IP address of 10.0.2.1 for all PTP packets.

```
switch(config)# ptp source ip 10.0.2.1
switch(config)#
```

Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 272.

See also Arista User Manual v. 4.12.3 (7/17/13), at 215.

Cisco NX-OS 6.2

Effective date of
registration:
11/13/2014**Configuration Examples for NTP**

This example shows how to configure an NTP server and peer, enable NTP authentication, enable NTP logging, and then save the configuration in startup so that it is saved across reboots and restarts:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ntp server 192.0.2.105 key 42
switch(config)# ntp peer 2001:db8::4101
switch(config)# show ntp peers
-----
Peer IP Address      Serv/Peer
-----
2001:db8::4101      Peer (configured)
192.0.2.105         Server (configured)
switch(config)# ntp authentication-key 42 md5 aNiceKey
switch(config)# show ntp authentication-keys
-----
Auth key      MD5 String
-----
42            aNicekey
switch(config)# ntp trusted-key 42
switch(config)# show ntp trusted-keys
Trusted Keys:
42
switch(config)# ntp authenticate
switch(config)# show ntp authentication-status
Authentication enabled.
switch(config)# ntp logging
switch(config)# show ntp logging
NTP logging enabled.
switch(config)# copy running-config startup-config
[*****] 100%
switch(config)#
```

Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 3-25.

Example

- These commands configure the switch to authenticate NTP packets using key 328 with the plaintext password "timeSync."

```
switch(config)# ntp authentication-key 328 md5 timeSync
switch(config)# ntp trusted key 328
switch(config)# ntp authenticate
switch(config)#
```

Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 270.

Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<table><tr><td>Step 4</td><td><code>[no] ptp domain number</code> Example: <code>switch(config)# ptp domain 1</code></td><td>(Optional) Configures the domain number to use for this clock. PTP domains allow you to use multiple independent PTP clocking subdomains on a single network. The range is from 0 to 128.</td></tr><tr><td>Step 5</td><td><code>[no] ptp priority1 value</code> Example: <code>switch(config)# ptp priority1 10</code></td><td>(Optional) Configures the priority1 value to use when advertising this clock. This value overrides the default criteria (clock quality, clock class, and so on) for best master clock selection. Lower values take precedence. The range is from 0 to 255.</td></tr><tr><td>Step 6</td><td><code>[no] ptp priority2 value</code> Example: <code>switch(config)# ptp priority2 20</code></td><td>(Optional) Configures the priority2 value to use when advertising this clock. This value is used to decide between two devices that are otherwise equally matched in the default criteria. For example, you can use the priority2 value to give a specific switch priority over other identical switches. The range is from 0 to 255.</td></tr><tr><td colspan="3"></td></tr></table>	Step 4	<code>[no] ptp domain number</code> Example: <code>switch(config)# ptp domain 1</code>	(Optional) Configures the domain number to use for this clock. PTP domains allow you to use multiple independent PTP clocking subdomains on a single network. The range is from 0 to 128.	Step 5	<code>[no] ptp priority1 value</code> Example: <code>switch(config)# ptp priority1 10</code>	(Optional) Configures the priority1 value to use when advertising this clock. This value overrides the default criteria (clock quality, clock class, and so on) for best master clock selection. Lower values take precedence. The range is from 0 to 255.	Step 6	<code>[no] ptp priority2 value</code> Example: <code>switch(config)# ptp priority2 20</code>	(Optional) Configures the priority2 value to use when advertising this clock. This value is used to decide between two devices that are otherwise equally matched in the default criteria. For example, you can use the priority2 value to give a specific switch priority over other identical switches. The range is from 0 to 255.				<p>ptp domain</p> <p>The ptp domain command configures the domain number to use for the clock. PTP domains allow you to use multiple independent PTP clocking subdomains on a single network. To remove PTP settings, use the no form of this command.</p> <p>Platform Arad, FM6000 Command Mode Global Configuration</p> <p>Command Syntax</p> <p><code>ptp domain domain number</code> <code>no ptp domain</code> <code>default ptp domain</code></p> <p>Parameters</p> <ul style="list-style-type: none"><code>domain_number</code> The domain number to use for the clock. Value ranges from 0 to 255. <p>Examples</p> <ul style="list-style-type: none">This command shows how to configure domain 1 for use with a clock. <code>switch(config)# ptp domain 1</code> <code>switch(config)#</code>This command removes the configured domain 1 for use with a clock. <code>switch(config)# no ptp domain 1</code> <code>switch(config)#</code>
	Step 4	<code>[no] ptp domain number</code> Example: <code>switch(config)# ptp domain 1</code>	(Optional) Configures the domain number to use for this clock. PTP domains allow you to use multiple independent PTP clocking subdomains on a single network. The range is from 0 to 128.											
	Step 5	<code>[no] ptp priority1 value</code> Example: <code>switch(config)# ptp priority1 10</code>	(Optional) Configures the priority1 value to use when advertising this clock. This value overrides the default criteria (clock quality, clock class, and so on) for best master clock selection. Lower values take precedence. The range is from 0 to 255.											
	Step 6	<code>[no] ptp priority2 value</code> Example: <code>switch(config)# ptp priority2 20</code>	(Optional) Configures the priority2 value to use when advertising this clock. This value is used to decide between two devices that are otherwise equally matched in the default criteria. For example, you can use the priority2 value to give a specific switch priority over other identical switches. The range is from 0 to 255.											
<p>Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 4-6.</p>			<p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 319.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 257; Arista User Manual, v. 4.11.1 (1/11/13), at 204.</p>											

Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<table><tr><td>Step 4</td><td><code>[no] ptp domain number</code> Example: <code>switch(config)# ptp domain 1</code></td><td>(Optional) Configures the domain number to use for this clock. PTP domains allow you to use multiple independent PTP clocking subdomains on a single network. The range is from 0 to 128.</td></tr><tr><td>Step 5</td><td><code>[no] ptp priority1 value</code> Example: <code>switch(config)# ptp priority1 10</code></td><td>(Optional) Configures the priority1 value to use when advertising this clock. This value overrides the default criteria (clock quality, clock class, and so on) for best master clock selection. Lower values take precedence. The range is from 0 to 255.</td></tr><tr><td>Step 6</td><td><code>[no] ptp priority2 value</code> Example: <code>switch(config)# ptp priority2 20</code></td><td>(Optional) Configures the priority2 value to use when advertising this clock. This value is used to decide between two devices that are otherwise equally matched in the default criteria. For example, you can use the priority2 value to give a specific switch priority over other identical switches. The range is from 0 to 255.</td></tr></table>	Step 4	<code>[no] ptp domain number</code> Example: <code>switch(config)# ptp domain 1</code>	(Optional) Configures the domain number to use for this clock. PTP domains allow you to use multiple independent PTP clocking subdomains on a single network. The range is from 0 to 128.	Step 5	<code>[no] ptp priority1 value</code> Example: <code>switch(config)# ptp priority1 10</code>	(Optional) Configures the priority1 value to use when advertising this clock. This value overrides the default criteria (clock quality, clock class, and so on) for best master clock selection. Lower values take precedence. The range is from 0 to 255.	Step 6	<code>[no] ptp priority2 value</code> Example: <code>switch(config)# ptp priority2 20</code>	(Optional) Configures the priority2 value to use when advertising this clock. This value is used to decide between two devices that are otherwise equally matched in the default criteria. For example, you can use the priority2 value to give a specific switch priority over other identical switches. The range is from 0 to 255.	<h3>ptp priority1</h3> <p>The <code>ptp priority1</code> command configures the priority1 value to use when advertising the clock. This value overrides the default criteria for best master clock selection. Lower values take precedence. The range is from 0 to 255. To remove PTP settings, use the no form of this command.</p> <table><tr><td>Platform</td><td>Arad, FM6000</td></tr><tr><td>Command Mode</td><td>Global Configuration</td></tr></table> <h4>Command Syntax</h4> <pre>ptp priority1 priority_rate no ptp priority1 default ptp priority1</pre> <h4>Parameters</h4> <ul style="list-style-type: none"><code>priority_rate</code> The value to override the default criteria (clock quality, clock class, etc.) for best master clock selection. Lower values take precedence. Value ranges from 0 to 255. The default is 128. <h4>Examples</h4> <ul style="list-style-type: none">This command configures the preference level for a clock; slave devices use the priority1 value when selecting a master clock.<pre>switch(config)# ptp priority1 120 switch(config)#</pre>This command removes the configured the preference level for a clock.<pre>switch(config)# no ptp priority1 switch(config)#</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 326.</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 318; Arista User Manual v. 4.12.3 (7/17/13), at 262; Arista User Manual, v. 4.11.1 (1/11/13), at 208.</p>	Platform	Arad, FM6000	Command Mode	Global Configuration
	Step 4	<code>[no] ptp domain number</code> Example: <code>switch(config)# ptp domain 1</code>	(Optional) Configures the domain number to use for this clock. PTP domains allow you to use multiple independent PTP clocking subdomains on a single network. The range is from 0 to 128.												
	Step 5	<code>[no] ptp priority1 value</code> Example: <code>switch(config)# ptp priority1 10</code>	(Optional) Configures the priority1 value to use when advertising this clock. This value overrides the default criteria (clock quality, clock class, and so on) for best master clock selection. Lower values take precedence. The range is from 0 to 255.												
	Step 6	<code>[no] ptp priority2 value</code> Example: <code>switch(config)# ptp priority2 20</code>	(Optional) Configures the priority2 value to use when advertising this clock. This value is used to decide between two devices that are otherwise equally matched in the default criteria. For example, you can use the priority2 value to give a specific switch priority over other identical switches. The range is from 0 to 255.												
Platform	Arad, FM6000														
Command Mode	Global Configuration														

<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<table border="1"> <tr> <td data-bbox="296 180 359 196">Step 4</td><td data-bbox="359 180 722 261"> <code>[no] ptp domain number</code> Example: <code>switch(config)# ptp domain 1</code> </td><td data-bbox="722 180 1142 261">(Optional) Configures the domain number to use for this clock. PTP domains allow you to use multiple independent PTP clocking subdomains on a single network. The range is from 0 to 128.</td></tr> <tr> <td data-bbox="296 269 359 285">Step 5</td><td data-bbox="359 269 722 350"> <code>[no] ptp priority1 value</code> Example: <code>switch(config)# ptp priority1 10</code> </td><td data-bbox="722 269 1142 350">(Optional) Configures the priority1 value to use when advertising this clock. This value overrides the default criteria (clock quality, clock class, and so on) for best master clock selection. Lower values take precedence. The range is from 0 to 255.</td></tr> <tr> <td data-bbox="296 391 359 407">Step 6</td><td data-bbox="359 391 722 472"> <code>[no] ptp priority2 value</code> Example: <code>switch(config)# ptp priority2 20</code> </td><td data-bbox="722 391 1142 472">(Optional) Configures the priority2 value to use when advertising this clock. This value is used to decide between two devices that are otherwise equally matched in the default criteria. For example, you can use the priority2 value to give a specific switch priority over other identical switches. The range is from 0 to 255.</td></tr> </table> <p>Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 4-6.</p>	Step 4	<code>[no] ptp domain number</code> Example: <code>switch(config)# ptp domain 1</code>	(Optional) Configures the domain number to use for this clock. PTP domains allow you to use multiple independent PTP clocking subdomains on a single network. The range is from 0 to 128.	Step 5	<code>[no] ptp priority1 value</code> Example: <code>switch(config)# ptp priority1 10</code>	(Optional) Configures the priority1 value to use when advertising this clock. This value overrides the default criteria (clock quality, clock class, and so on) for best master clock selection. Lower values take precedence. The range is from 0 to 255.	Step 6	<code>[no] ptp priority2 value</code> Example: <code>switch(config)# ptp priority2 20</code>	(Optional) Configures the priority2 value to use when advertising this clock. This value is used to decide between two devices that are otherwise equally matched in the default criteria. For example, you can use the priority2 value to give a specific switch priority over other identical switches. The range is from 0 to 255.	<p>ptp priority2</p> <p>The <code>ptp priority2</code> command configures the priority2 value to use when advertising this clock. This value is used to decide between two devices that are otherwise equally matched in the default criteria. For example, you can use the priority2 value to give a specific switch priority over other identical switches. The range is from 0 to 255. To remove PTP settings, use the no form of this command.</p> <p>Platform Arad, FM6000 Command Mode Global Configuration</p> <p>Command Syntax</p> <pre>ptp priority2 priority_rate no ptp priority2 default ptp priority2</pre> <p>Parameters</p> <ul style="list-style-type: none"> <i>priority_rate</i> Sets a secondary preference level for a clock; slave devices use the priority2 value when selecting a master clock. Value ranges from 0 to 255. <p>Examples</p> <ul style="list-style-type: none"> This command sets a secondary preference level for a clock to 128. <pre>switch(config)# ptp priority2 128 switch(config)#</pre> This command removes the secondary preference level for a clock. <pre>switch(config)# no ptp priority2 switch(config)#</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 327.</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 319; Arista User Manual v. 4.12.3 (7/17/13), at 263; Arista User Manual, v. 4.11.1 (1/11/13), at 209.</p>
Step 4	<code>[no] ptp domain number</code> Example: <code>switch(config)# ptp domain 1</code>	(Optional) Configures the domain number to use for this clock. PTP domains allow you to use multiple independent PTP clocking subdomains on a single network. The range is from 0 to 128.									
Step 5	<code>[no] ptp priority1 value</code> Example: <code>switch(config)# ptp priority1 10</code>	(Optional) Configures the priority1 value to use when advertising this clock. This value overrides the default criteria (clock quality, clock class, and so on) for best master clock selection. Lower values take precedence. The range is from 0 to 255.									
Step 6	<code>[no] ptp priority2 value</code> Example: <code>switch(config)# ptp priority2 20</code>	(Optional) Configures the priority2 value to use when advertising this clock. This value is used to decide between two devices that are otherwise equally matched in the default criteria. For example, you can use the priority2 value to give a specific switch priority over other identical switches. The range is from 0 to 255.									
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>BEFORE YOU BEGIN</p> <p>Make sure that you are in the correct VDC. To change the VDC, use the <code>switchto vdc</code> command. Make sure that you have globally enabled PTP on the device and configured the source IP address for PTP communication.</p> <p>Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 4-7.</p>	<p>ptp delay-req interval</p> <p>The <code>ptp delay-req interval</code> command specifies the time recommended to the slave devices to send delay request messages. You must enable PTP on the switch first and configure the source IP address for PTP communication. To remove the minimum interval configuration for PTP delay-request messages, use the no form of this command.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 318.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 256; Arista User Manual, v. 4.11.1 (1/11/13), at 202.</p>									

<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>Step 4 <code>[no] ptp announce {interval seconds timeout count}</code></p> <p>Example: <code>switch(config-if)# ptp announce interval 1</code></p> <p>Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 4-8.</p>	<p>ptp announce interval</p> <p>The <code>ptp announce interval</code> command configures the interval between PTP announcement messages on or the number of PTP intervals before a timeout occurs. To disable this feature, use the no form of this command.</p> <p>Platform Arad, FM6000 Command Mode Interface-Ethernet Configuration Interface-Port Channel Configuration</p> <p>Command Syntax</p> <pre>ptp announce interval log_interval no ptp announce interval default ptp announce interval</pre> <p>Parameters</p> <ul style="list-style-type: none"><code>log_interval</code> The number of log seconds between PTP announcement message (base 2 log (seconds)). Value ranges from 0 to 4; default value is 1. <p>Examples</p> <ul style="list-style-type: none">This command shows how to configure the interval between PTP announce messages on an interface. <pre>switch(config)# interface ethernet 5 switch(config-if-Et5)# ptp announce interval 1 switch(config-if-Et5)#</pre>This command removes the configured interval between PTP announce messages on interface Ethernet 5. <pre>switch(config)# interface ethernet 5 switch(config-if-Et5)# no ptp announce interval switch(config-if-Et5)#</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 315.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 252; Arista User Manual, v. 4.11.1 (1/11/13), at 199.</p>
--	--	---

Step 5 [no] **ptp delay-request minimum interval**
seconds

Example:
switch(config-if)# ptp delay-request minimum
interval 3

(Optional) Configures the minimum interval allowed between PTP delay-request messages when the port is in the master state. The range is from -1 to 6 seconds.

Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 4-8.

ptp delay-req interval

The ptp delay-req interval command specifies the time recommended to the slave devices to send delay request messages. You must enable PTP on the switch first and configure the source IP address for PTP communication. To remove the minimum interval configuration for PTP delay-request messages, use the no form of this command.

Platform Arad, FM6000
Command Mode Interface-Ethernet Configuration
Interface-Port Channel Configuration

Command Syntax

```
ptp delay-req interval log_interval
no ptp delay-req interval
default ptp delay-req interval
```

Parameters

- *log_interval* The range is -1 second to 8 seconds. The default is 5 log(seconds).

Examples

- This command shows how to configure the minimum interval allowed between PTP delay-request messages.

```
switch(config)# interface ethernet 5
switch(config-if-Et5)# ptp delay-request interval 3
switch(config-if-Et5)#
```

- This command removes the configured minimum interval allowed between PTP delay-request messages.

```
switch(config)# interface ethernet 5
switch(config-if-Et5)# no ptp delay-request interval
switch(config-if-Et5)#
```

Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 318.

See also Arista User Manual v. 4.12.3 (7/17/13), at 256; Arista User Manual, v. 4.11.1 (1/11/13), at 202.

Cisco NX-OS 6.2

Effective date of
registration:
11/13/2014

Verifying the PTP Configuration

To display the PTP configuration, perform one of the following tasks:

Command	Purpose
<code>show ptp brief</code>	Displays the PTP status.
<code>show ptp clock</code>	Displays the properties of the local clock.
<code>show ptp clock foreign-masters record [interface interface slot/port]</code>	Displays the state of foreign masters known to the PTP process. For each foreign master, the output displays the clock identity, basic clock properties, and whether the clock is being used as a grandmaster.
<code>show ptp corrections</code>	Displays the last few PTP corrections.
<code>show ptp parent</code>	Displays the properties of the PTP parent.
<code>show ptp port interface interface slot/port</code>	Displays the status of the PTP port.
<code>show ptp time-property</code>	Displays the properties of the PTP clock.

Cisco NX-OS 6.2

Effective date of
registration:
11/13/2014

Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 4-9.

show ptp foreign-master-record

The `show ptp foreign-master-record` command displays information about the state of foreign masters known to the Precision Time Protocol (PTP) process.

Platform Arad, FM6000
Command Mode EXEC

Command Syntax

show ptp foreign-master-record

Examples

- This command shows how to display information about the state of foreign masters known to the PTP process.

```
switch# show ptp clocks foreign-masters-record
No Foreign Master Records
switch#
```

Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 349.

See also Arista User Manual v. 4.12.3 (7/17/13), at 282; Arista User Manual, v. 4.11.1 (1/11/13), at 228.

<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>SNMP Functional Overview</p> <p>The SNMP framework consists of three parts:</p> <ul style="list-style-type: none"> • An SNMP manager—The system used to control and monitor the activities of network devices using SNMP. • An SNMP agent—The software component within the managed device that maintains the data for the device and reports these data, as needed, to managing systems. Cisco NX-OS supports the agent and MIB. To enable the SNMP agent, you must define the relationship between the manager and the agent. • A managed information base (MIB)—The collection of managed objects on the SNMP agent. <p>SNMP is defined in RFCs 3411 to 3418.</p> <p>Cisco NX-OS supports SNMPv1, SNMPv2c, and SNMPv3. Both SNMPv1 and SNMPv2c use a community-based form of security.</p> <p>Cisco NX-OS supports SNMP over IPv6.</p> <p>Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 11-2.</p>	<p>37.2.3 SNMP Versions</p> <p>Arista switches support the following SNMP versions:</p> <ul style="list-style-type: none"> • SNMPv1: The Simple Network Management Protocol, defined in RFC 1157. Security is based on community strings. • SNMPv2c: Community-string based Administrative Framework for SNMPv2, defined in RFC 1901 RFC 1905, and RFC 1906. SNMPv2c uses the community-based security model of SNMPv1. • SNMPv3: Version 3 is an interoperable standards-based protocol defined in RFCs 2273 to 2275. SNMPv3 provides secure access to devices by authenticating and encrypting packets. <p>The security features provided in SNMPv3 are as follows:</p> <ul style="list-style-type: none"> — <i>Message integrity:</i> Ensures packets are not tampered with in transit. — <i>Authentication:</i> Determines the message is received from a valid source. — <i>Encryption:</i> Scrambling packet contents to prevent an unauthorized source from learning it. <p>Both SNMPv1 and SNMPv2c use a community-based form of security. The community of managers able to access the agent MIB is controlled by a password.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 349.</p> <p><i>See also</i> Arista User Manual v. 4.13.6F (4/14/2014), at 1891; Arista User Manual v. 4.12.3 (7/17/13), at 1654; Arista User Manual, v. 4.11.1 (1/11/13), at 1341; Arista User Manual v. 4.10.3 (10/22/12), at 1107; Arista User Manual v. 4.9.3.2 (5/3/12), at 863; Arista User Manual v. 4.8.2 (11/18/11), at 675; Arista User Manual v. 4.7.3 (7/18/11), at 531.</p>
--	---	--

<p>Cisco NX-OS 5.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>SNMP Functional Overview</p> <p>The SNMP framework consists of three parts:</p> <ul style="list-style-type: none"> • An SNMP manager—The system used to control and monitor the activities of network devices using SNMP. • An SNMP agent—The software component within the managed device that maintains the data for the device and reports these data, as needed, to managing systems. Cisco NX-OS supports the agent and MIB. To enable the SNMP agent, you must define the relationship between the manager and the agent. • A managed information base (MIB)—The collection of managed objects on the SNMP agent. <p>SNMP is defined in RFCs 3411 to 3418.</p> <p>Cisco NX-OS supports SNMPv1, SNMPv2c, and SNMPv3. Both SNMPv1 and SNMPv2c use a community-based form of security.</p> <p>Cisco NX-OS supports SNMP over IPv6.</p> <p>Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 5.x (2010), at 10-2.</p>	<p>37.2.3 SNMP Versions</p> <p>Arista switches support the following SNMP versions:</p> <ul style="list-style-type: none"> • SNMPv1: The Simple Network Management Protocol, defined in RFC 1157. Security is based on community strings. • SNMPv2c: Community-string based Administrative Framework for SNMPv2, defined in RFC 1901 RFC 1905, and RFC 1906. SNMPv2c uses the community-based security model of SNMPv1. • SNMPv3: Version 3 is an interoperable standards-based protocol defined in RFCs 2273 to 2275. SNMPv3 provides secure access to devices by authenticating and encrypting packets. <p>The security features provided in SNMPv3 are as follows:</p> <ul style="list-style-type: none"> — <i>Message integrity:</i> Ensures packets are not tampered with in transit. — <i>Authentication:</i> Determines the message is received from a valid source. — <i>Encryption:</i> Scrambling packet contents to prevent an unauthorized source from learning it. <p>Both SNMPv1 and SNMPv2c use a community-based form of security. The community of managers able to access the agent MIB is controlled by a password.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 349.</p> <p><i>See also</i> Arista User Manual v. 4.13.6F (4/14/2014), at 1891; Arista User Manual v. 4.12.3 (7/17/13), at 1654; Arista User Manual, v. 4.11.1 (1/11/13), at 1341; Arista User Manual v. 4.10.3 (10/22/12), at 1107; Arista User Manual v. 4.9.3.2 (5/3/12), at 863; Arista User Manual v. 4.8.2 (11/18/11), at 675; Arista User Manual v. 4.7.3 (7/18/11), at 531.</p>
--	---	--

<p>Cisco NX-OS 4.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>Cisco NX-OS supports SNMPv1, SNMPv2c and SNMPv3. Both SNMPv1 and SNMPv2c use a community-based form of security.</p> <p>Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 4.0 (2008), at 10-2.</p>	<p>37.2.3 SNMP Versions</p> <p>Arista switches support the following SNMP versions:</p> <ul style="list-style-type: none"> • SNMPv1: The Simple Network Management Protocol, defined in RFC 1157. Security is based on community strings. • SNMPv2c: Community-string based Administrative Framework for SNMPv2, defined in RFC 1901 RFC 1905, and RFC 1906. SNMPv2c uses the community-based security model of SNMPv1. • SNMPv3: Version 3 is an interoperable standards-based protocol defined in RFCs 2273 to 2275. SNMPv3 provides secure access to devices by authenticating and encrypting packets. <p>The security features provided in SNMPv3 are as follows:</p> <ul style="list-style-type: none"> — <i>Message integrity:</i> Ensures packets are not tampered with in transit. — <i>Authentication:</i> Determines the message is received from a valid source. — <i>Encryption:</i> Scrambling packet contents to prevent an unauthorized source from learning it. <p>Both SNMPv1 and SNMPv2c use a community-based form of security. The community of managers able to access the agent MIB is controlled by a password.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 349.</p> <p><i>See also</i> Arista User Manual v. 4.13.6F (4/14/2014), at 1891; Arista User Manual v. 4.12.3 (7/17/13), at 1654; Arista User Manual, v. 4.11.1 (1/11/13), at 1341; Arista User Manual v. 4.10.3 (10/22/12), at 1107; Arista User Manual v. 4.9.3.2 (5/3/12), at 863; Arista User Manual v. 4.8.2 (11/18/11), at 675; Arista User Manual v. 4.7.3 (7/18/11), at 531.</p>
--	--	---

SNMPv3

SNMPv3 provides secure access to devices by a combination of authenticating and encrypting frames over the network. The security features provided in SNMPv3 are as follows:

- **Message integrity**—Ensures that a packet has not been tampered with while it was in-transit.
- **Authentication**—Determines that the message is from a valid source.
- **Encryption**—Scrambles the packet contents to prevent it from being seen by unauthorized sources.

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the role in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet.

This section includes the following topics:

- [Security Models and Levels for SNMPv1, v2, v3, page 11-4](#)
- [User-Based Security Model, page 11-5](#)
- [CLI and SNMP User Synchronization, page 11-5](#)

Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 11-3.

Cisco NX-OS 6.2

Effective date of
registration:
11/13/2014

37.2.3 SNMP Versions

Arista switches support the following SNMP versions:

- **SNMPv1:** The Simple Network Management Protocol, defined in RFC 1157. Security is based on community strings.
- **SNMPv2c:** Community-string based Administrative Framework for SNMPv2, defined in RFC 1901, RFC 1905, and RFC 1906. SNMPv2c uses the community-based security model of SNMPv1.
- **SNMPv3:** Version 3 is an interoperable standards-based protocol defined in RFCs 2273 to 2275. SNMPv3 provides secure access to devices by authenticating and encrypting packets.

The security features provided in SNMPv3 are as follows:

- **Message integrity:** Ensures packets are not tampered with in transit.
- **Authentication:** Determines the message is received from a valid source.
- **Encryption:** Scrambling packet contents to prevent an unauthorized source from learning it.

Both SNMPv1 and SNMPv2c use a community-based form of security. The community of managers able to access the agent MIB is controlled by a password.

SNMPv2c support includes a bulk retrieval mechanism and more detailed error message reporting. The bulk retrieval mechanism supports the retrieval of tables and large quantities of information, minimizing the number of round-trips required. SNMPv2c error handling includes expanded error codes that distinguish different kinds of error conditions; these conditions are reported through a single error code in SNMPv1. SNMPv2c error return codes report error type.

SNMPv3 is a security model which defines an authentication strategy that is configured for a user and the group in which the user resides. A security level is the permitted level of security within the model. A combination of a security model and a security level determines the security mechanism employed to handle an SNMP packet.

Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 349.

See also Arista User Manual v. 4.13.6F (4/14/2014), at 1891; Arista User Manual v. 4.12.3 (7/17/13), at 1654; Arista User Manual, v. 4.11.1 (1/11/13), at 1341; Arista User Manual v. 4.10.3 (10/22/12), at 1107-08; Arista User Manual v. 4.9.3.2 (5/3/12), at 863; Arista User Manual v. 4.7.3 (7/18/11), at 531.

SNMPv3

SNMPv3 provides secure access to devices by a combination of authenticating and encrypting frames over the network. The security features provided in SNMPv3 are as follows:

- **Message integrity**—Ensures that a packet has not been tampered with while it was in-transit.
- **Authentication**—Determines that the message is from a valid source.
- **Encryption**—Scrambles the packet contents to prevent it from being seen by unauthorized sources.

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the role in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet.

Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 5.x (2010), at 10-2.

Cisco NX-OS 5.0

Effective date of
registration:
11/13/2014

37.2.3 SNMP Versions

Arista switches support the following SNMP versions:

- **SNMPv1:** The Simple Network Management Protocol, defined in RFC 1157. Security is based on community strings.
- **SNMPv2c:** Community-string based Administrative Framework for SNMPv2, defined in RFC 1901, RFC 1905, and RFC 1906. SNMPv2c uses the community-based security model of SNMPv1.
- **SNMPv3:** Version 3 is an interoperable standards-based protocol defined in RFCs 2273 to 2275. SNMPv3 provides secure access to devices by authenticating and encrypting packets.

The security features provided in SNMPv3 are as follows:

- **Message integrity:** Ensures packets are not tampered with in transit.
- **Authentication:** Determines the message is received from a valid source.
- **Encryption:** Scrambling packet contents to prevent an unauthorized source from learning it.

Both SNMPv1 and SNMPv2c use a community-based form of security. The community of managers able to access the agent MIB is controlled by a password.

SNMPv2c support includes a bulk retrieval mechanism and more detailed error message reporting. The bulk retrieval mechanism supports the retrieval of tables and large quantities of information, minimizing the number of round-trips required. SNMPv2c error handling includes expanded error codes that distinguish different kinds of error conditions; these conditions are reported through a single error code in SNMPv1. SNMPv2c error return codes report error type.

SNMPv3 is a security model which defines an authentication strategy that is configured for a user and the group in which the user resides. A security level is the permitted level of security within the model. A combination of a security model and a security level determines the security mechanism employed to handle an SNMP packet.

Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 349.

See also Arista User Manual v. 4.13.6F (4/14/2014), at 1891; Arista User Manual v. 4.12.3 (7/17/13), at 1654; Arista User Manual, v. 4.11.1 (1/11/13), at 1341; Arista User Manual v. 4.10.3 (10/22/12), at 1107-08; Arista User Manual v. 4.9.3.2 (5/3/12), at 863; Arista User Manual v. 4.7.3 (7/18/11), at 531.

<p>Cisco NX-OS 4.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>SNMPv3</p> <p>SNMPv3 provides secure access to devices by a combination of authenticating and encrypting frames over the network. The security features provided in SNMPv3 are as follows:</p> <ul style="list-style-type: none"> • Message integrity—Ensures that a packet has not been tampered with while it was in-transit. • Authentication—Determines that the message is from a valid source. • Encryption—Scrambles the packet contents to prevent it from being seen by unauthorized sources. <p>SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the role in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet.</p> <p>Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 4.0 (2008), at 7-2.</p>	<p>37.2.3 SNMP Versions</p> <p>Arista switches support the following SNMP versions:</p> <ul style="list-style-type: none"> • SNMPv1: The Simple Network Management Protocol, defined in RFC 1157. Security is based on community strings. • SNMPv2c: Community-string based Administrative Framework for SNMPv2, defined in RFC 1901, RFC 1905, and RFC 1906. SNMPv2c uses the community-based security model of SNMPv1. • SNMPv3: Version 3 is an interoperable standards-based protocol defined in RFCs 2273 to 2275. SNMPv3 provides secure access to devices by authenticating and encrypting packets. <p>The security features provided in SNMPv3 are as follows:</p> <ul style="list-style-type: none"> — Message integrity: Ensures packets are not tampered with in transit. — Authentication: Determines the message is received from a valid source. — Encryption: Scrambling packet contents to prevent an unauthorized source from learning it. <p>Both SNMPv1 and SNMPv2c use a community-based form of security. The community of managers able to access the agent MIB is controlled by a password.</p> <p>SNMPv2c support includes a bulk retrieval mechanism and more detailed error message reporting. The bulk retrieval mechanism supports the retrieval of tables and large quantities of information, minimizing the number of round-trips required. SNMPv2c error handling includes expanded error codes that distinguish different kinds of error conditions; these conditions are reported through a single error code in SNMPv1. SNMPv2c error return codes report error type.</p> <p>SNMPv3 is a security model which defines an authentication strategy that is configured for a user and the group in which the user resides. A security level is the permitted level of security within the model. A combination of a security model and a security level determines the security mechanism employed to handle an SNMP packet.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 349.</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 1891; Arista User Manual v. 4.12.3 (7/17/13), at 1654; Arista User Manual, v. 4.11.1 (1/11/13), at 1341; Arista User Manual v. 4.10.3 (10/22/12), at 1107-08; Arista User Manual v. 4.9.3.2 (5/3/12), at 863; Arista User Manual v. 4.7.3 (7/18/11), at 531.</p>
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>SNMPv3 uses contexts to distinguish between these multiple instances. An SNMP context is a collection of management information that you can access through the SNMP agent. A device can support multiple contexts for different logical network entities. An SNMP context allows the SNMP manager to access one of the multiple instances of a MIB module supported on the device for the different logical network entities.</p> <p>Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 11-3.</p>	<p>An SNMP context is a collection of management information items accessible by an SNMP entity. Each item of may exist in multiple contexts. Each SNMP entity can access multiple contexts. A context is identified by the EngineID of the hosting device and a context name.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 1994.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1684; Arista User Manual, v. 4.11.1 (1/11/13), at 1369; Arista User Manual v. 4.10.3 (10/22/12), at 1136; Arista User Manual v. 4.9.3.2 (5/3/12), at 892; Arista User Manual v. 4.8.2 (11/18/11), at 699; Arista User Manual v. 4.7.3 (7/18/11), at 555.</p>

<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>Step 2 <code>vlan vlan</code></p> <p>Examples:</p> <pre>switch(config)# vlan 901 switch(config-vlan)#</pre> <p>Enters VLAN configuration mode for the VLAN specified.</p> <p>Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 16-18.</p>	<p>Example</p> <ul style="list-style-type: none"> This command creates VLAN 49 and enters VLAN configuration mode for the new VLAN: <pre>switch(config)#vlan 49 switch(config-vlan-49)#</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 803.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 650; Arista User Manual, v. 4.11.1 (1/11/13), at 502; Arista User Manual v. 4.10.3 (10/22/12), at 420; Arista User Manual v. 4.9.3.2 (5/3/12), at 359.</p>
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>To permit the discovery of non-Cisco devices, the switch also supports the <i>Link Layer Discovery Protocol (LLDP)</i>, a vendor-neutral device discovery protocol that is defined in the IEEE 802.1ab standard. LLDP allows network devices to advertise information about themselves to other devices on the network. This protocol runs over the data-link layer, which allows two systems running different network layer protocols to learn about each other.</p> <p>Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 18-2.</p>	<p>Link Layer Discovery Protocol (LLDP) allows Ethernet network devices to advertise details about themselves, such as device configuration, capabilities and identification, to directly connected devices on the network that are also using LLDP.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 572.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 447; Arista User Manual, v. 4.11.1 (1/11/13), at 365.</p>
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>Guidelines and Limitations</p> <p>LLDP has the following configuration guidelines and limitations:</p> <ul style="list-style-type: none"> • LLDP must be enabled on the device before you can enable or disable it on any interfaces. • LLDP is supported only on physical interfaces. • LLDP can discover up to one device per port. • LLDP can discover Linux servers, provided they are not using a converged network adapter (CNA). LLDP cannot discover other types of servers. • DCBXP incompatibility messages might appear when you change the network QoS policy, if a physical loopback connection is in the device. The incompatibility exists for only a short time and then clears. • DCBXP is not supported for the Cisco Nexus 2000 Series Fabric Extender. • Beginning with Cisco NX-OS Release 5.2, LLDP is supported for the Cisco Nexus 2000 Series Fabric Extender. LLDP packets can now be sent and received through the Fabric Extender ports for neighbor discovery. <ul style="list-style-type: none"> – All LLDP configuration on Fabric Extender ports occurs on the supervisor. LLDP configuration and show commands are not visible on the Fabric Extender console. – LLDP is not supported for a Fabric Extender-virtual port channel (vPC) connection. <p>Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 18-2.</p>	<p>12.2.4 Guidelines and Limitations</p> <p>LLDP has the following configuration guidelines and limitations:</p> <ul style="list-style-type: none"> • LLDP must be enabled on the device before you can enable or disable it on any interface. • LLDP is supported only on physical interfaces. • LLDP can discover up to one device per port. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 576.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 448; Arista User Manual, v. 4.11.1 (1/11/13), at 366.</p>

Cisco NX-OS 6.2

Effective date of
registration:
11/13/2014

Enabling or Disabling LLDP on an Interface

After you globally enable LLDP, it is enabled on all supported interfaces by default. However, you can enable or disable LLDP on individual interfaces or selectively configure an interface to only send or only receive LLDP packets.



Note

If the interface is configured as a tunnel port, LLDP is disabled automatically.

BEFORE YOU BEGIN

Make sure that you are in the correct VDC. To switch VDCs, use the `switchto vdc` command.
Make sure that you have globally enabled LLDP on the device.

SUMMARY STEPS

1. `config t`
2. `interface ethernet slot/port`
3. `[no] lldp transmit`
4. `[no] lldp receive`
5. (Optional) `show lldp interface ethernet slot/port`
6. (Optional) `copy running-config startup-config`

DETAILED STEPS

	Command	Purpose
Step 1	<code>config t</code> Example: <code>switch# config t</code> Enter configuration commands, one per line. End with <code>CNTL/Z</code> . <code>switch(config)#</code>	Enters global configuration mode.
Step 2	<code>interface ethernet slot/port</code> Example: <code>switch(config)# interface ethernet 7/1</code> <code>switch(config-if)</code>	Specifies the interface on which you are enabling LLDP and enters the interface configuration mode.
Step 3	<code>[no] lldp transmit</code> Example: <code>switch(config-if)# lldp transmit</code>	Enables or disables the transmission of LLDP packets on an interface. After you globally enable LLDP, it is enabled on all supported interfaces by default.
Step 4	<code>[no] lldp receive</code> Example: <code>switch(config-if)# lldp receive</code>	Enables or disables the reception of LLDP packets on an interface. After you globally enable LLDP, it is enabled on all supported interfaces by default.

Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 18-6.

12.3.2 Enabling LLDP on an Interface

After you globally enable LLDP, it is enabled on all supported interfaces by default. However, by using the `lldp transmit` and `lldp receive` commands, you can enable or disable LLDP on individual interfaces or selectively configure an interface to only send or only receive LLDP packets.

Examples

- These commands enable Ethernet port 3/1 to transmit LLDP packets.
`switch(config)# interface ethernet 3/1`
`switch(config-if-Et3/1)# lldp transmit`
`switch(config-if-Et3/1)#`
- These commands enable Ethernet port 3/1 to receive LLDP packets.
`switch(config)# interface ethernet 3/1`
`switch(config-if-Et3/1)# lldp receive`
`switch(config-if-Et3/1)#`

Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 577.

See also Arista User Manual v. 4.12.3 (7/17/13), at 449; Arista User Manual, v. 4.11.1 (1/11/13), at 367.

<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<div><div><div>Step 3</div><div><div>[no] lldp transmit</div><div>Example: switch(config-if)# lldp transmit</div></div></div><div><div>Enables or disables the transmission of LLDP packets on an interface. After you globally enable LLDP, it is enabled on all supported interfaces by default.</div></div></div> <p>Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 18-6.</p>	<h3>lldp transmit</h3> <p>The lldp transmit command enables the transmission of LLDP packets on an interface. After you globally enable LLDP, it is enabled on all supported interfaces by default.</p> <table><tr><td>Platform</td><td>all</td></tr><tr><td>Command Mode</td><td>Interface-Ethernet configuration Interface-Management configuration</td></tr></table> <p>Command Syntax</p> <pre>lldp transmit no lldp transmit default lldp transmit</pre> <p>Examples</p> <ul style="list-style-type: none">These commands enable the transmission of LLDP packets on a specific interface.<pre>switch(config)#interface ethernet 4/1 switch(config-if-Et4/1)#lldp transmit switch(config-if-Et4/1)#</pre>These commands disable the transmission of LLDP packets on a specific interface.<pre>switch(config)#interface ethernet 4/1 switch(config-if-Et4/1)#no lldp transmit switch(config-if-Et4/1)#</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 593.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 466; Arista User Manual, v. 4.11.1 (1/11/13), at 384.</p>	Platform	all	Command Mode	Interface-Ethernet configuration Interface-Management configuration
	Platform	all				
Command Mode	Interface-Ethernet configuration Interface-Management configuration					

<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>Step 4 [no] lldp receive</p> <p>Example: Switch(config-if)# lldp receive</p> <p>Enables or disables the reception of LLDP packets on an interface. After you globally enable LLDP, it is enabled on all supported interfaces by default.</p> <p>Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 18-6.</p>	<p>lldp receive</p> <p>The lldp receive command enables the reception of LLDP packets on an interface. After you globally enable LLDP, it is enabled on all supported interfaces by default. The no form of the is command disables the reception of LLDP packets on an interface.</p> <p>Platform all Command Mode Interface-Ethernet configuration Interface-Management configuration</p> <p>Command Syntax</p> <pre>lldp receive no lldp receive default lldp receive</pre> <p>Examples</p> <ul style="list-style-type: none"> These commands enables the reception of LLDP packets on a specific interface. <pre>switch(config)#interface ethernet 4/1 switch(config-if-Et4/1)#lldp receive switch(config-if-Et4/1)#</pre> <ul style="list-style-type: none"> These commands disables LLDP the reception of LLDP packets on a specific interface. <pre>switch(config)#interface ethernet 4/1 switch(config-if-Et4/1)# no lldp receive switch(config-if-Et4/1)#</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 588.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 461; Arista User Manual, v. 4.11.1 (1/11/13), at 379.</p>
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>Configuring Optional LLDP Parameters</p> <p>You can configure the frequency of LLDP updates, the amount of time for a receiving device to hold the information before discarding it, and the initialization delay time. You can also select the TLVs to include in LLDP packets.</p> <p>Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 18-7.</p>	<p>12.3.3 Optional LLDP Parameters</p> <p>You can globally configure the frequency of LLDP updates, the amount of time for a receiving device to hold the information before discarding it, and the initialization delay time. You can also select the TLVs to include in LLDP packets.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 577.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 449; Arista User Manual, v. 4.11.1 (1/11/13), at 367.</p>

<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<div data-bbox="302 173 709 253"> <p>Step 2 [no] lldp holdtime <i>seconds</i></p> <p>Example: switch(config)# lldp holdtime 200</p> </div> <div data-bbox="747 173 1129 289"> <p>(Optional) Specifies the amount of time in seconds that a receiving device should hold the information sent by your device before discarding it.</p> <p>The range is 10 to 255 seconds; the default is 120 seconds.</p> </div> <p>Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 18-8.</p>	<p>12.3.3.2 Setting the LLDP Hold Time</p> <p>The lldp holdtime command specifies the amount of time in seconds that a receiving device should hold the information sent by the device before discarding it.</p> <p>Examples</p> <ul style="list-style-type: none"> This command specifies that the receiving device should retain the information for 180 seconds before discarding it. switch(config)# lldp holdtime 180 switch(config)# This command reverts the LLDP hold time and to the default value of 120 seconds. switch(config)# no lldp holdtime 180 switch(config)# <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 578.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 450; Arista User Manual, v. 4.11.1 (1/11/13), at 368.</p>
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<div data-bbox="302 651 709 740"> <p>[no] lldp reinit <i>seconds</i></p> <p>Example: switch(config)# lldp reinit 5</p> </div> <div data-bbox="709 651 1129 764"> <p>(Optional) Specifies the delay time in seconds for LLDP to initialize on any interface.</p> <p>The range is 1 to 10 seconds; the default is 2 seconds.</p> </div> <p>Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 18-8.</p>	<p>lldp reinit</p> <p>The lldp reinit command specifies the delay time in seconds for LLDP to initialize on any interface.</p> <p>Platform all Command Mode Global Configuration</p> <p>Command Syntax</p> <p>lldp reinit <i>delay</i> no lldp reinit default lldp reinit</p> <p>Parameters</p> <ul style="list-style-type: none"> <i>delay</i> the amount of time the device should wait before re-initialization is attempted. Value ranges from 1 to 20 seconds; default value is 2 seconds. <p>Examples</p> <ul style="list-style-type: none"> This command specifies that the switch should wait 10 seconds before attempting to re-initialize. switch(config)# lldp reinit 10 switch(config)# This command removes the re-initialize timer. switch(config)# no lldp reinit 10 switch(config)# <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 589.</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 318; Arista User Manual v. 4.12.3 (7/17/13), at 262; Arista User Manual, v. 4.11.1 (1/11/13), at 208.</p>

Cisco NX-OS 6.2

Effective date of registration:
11/13/2014

Step 6	<code>[no] lldp tlv-select tlv</code>	(Optional) Specifies the TLVs to send and receive in LLDP packets. The available TLVs are dcbxp, management-address, port-description, port-vlan, system-capabilities, system-description, and system-name. All available TLVs are enabled by default.
	Example: <code>switch(config)# lldp tlv-select system-name</code>	Note For more information about using these TLVs, see the <i>Cisco Nexus 7000 Series NX-OS System Management Command Reference</i> .

Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 18-8.

lldp tlv-select

The `lldp tlv-select` command allows the user to specify the TLVs to send and receive in LLDP packets. The available TLVs are management-address, port-description, port-vlan, system-capabilities, system-description, and system-name.

Platform all
Command Mode Global Configuration

Command Syntax

```
lldp tlv-select TLV_NAME
no lldp tlv-select TLV_NAME
default lldp tlv-select TLV_NAME
```

Parameters

- *TLV_NAME* the TLV specifies the information to be sent or received in the LLDP packet: Options include:
 - link-aggregation specifies the link aggregation TLV.
 - management-address specifies the management address TLV.
 - max-frame-size specifies the Frame size TLV.
 - port-description specifies the port description TLV.
 - port-vlan specifies the port VLAN ID TLV.
 - system-capabilities specifies the system capabilities TLV.
 - system-description specifies the system description TLV.
 - system-name specifies the system name TLV.

Example

- This command enables the system description TLV:

```
switch(config)# lldp tlv-select system-description
switch(config)#
```
- This command disables the system description TLV:

```
switch(config)# no lldp tlv-select system-description
switch(config)#
```
- This command enables the max-frame-size TLV:

```
switch(config)# lldp tlv-select max-frame-size
switch(config)#
```
- This command disables the max-frame-size TLV:

```
switch(config)# no lldp tlv-select max-frame-size
switch(config)#
```

Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 592.

See also Arista User Manual v. 4.12.3 (7/17/13), at 465; Arista User Manual, v. 4.11.1 (1/11/13), at 383.

<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<div data-bbox="302 175 716 277"> <p><code>show lldp traffic</code></p> </div> <div data-bbox="716 175 1142 277"> <p>Displays the LLDP counters, including the number of LLDP packets sent and received by the device, the number of discarded packets, and the number of unrecognized TLVs.</p> </div> <p>Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 18-9.</p>	<p>12.3.5.4 Viewing LLDP Traffic</p> <p>The <code>show lldp traffic</code> command displays the LLDP counters, including the number of packets sent and received, and the number of packets discarded by the switch.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 581.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 454; Arista User Manual, v. 4.11.1 (1/11/13), at 372.</p>
--	--	---

Month	Number of Visitors
January	10
February	20
March	30
April	40
May	50
June	60
July	70
August	80
September	90
October	100
November	95
December	85

-2-

-3-

-4-

-5-

-6-

-7-

-8-

-9-

-10-

-11-

-12-

-13-

-14- CASE No. 5:14-cv-05344-BLF
EXHIBIT G TO CISCO'S OBJECTIONS AND RESPONSES TO ARISTA'S FIRST SET OF INTERROGATORIES

-15-

-16-

-17-

-18-

[illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

HIGHLY CONFIDENTIAL – SOURCE CODE

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

HIGHLY CONFIDENTIAL – SOURCE CODE

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

HIGHLY CONFIDENTIAL – SOURCE CODE

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

HIGHLY CONFIDENTIAL – SOURCE CODE

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

HIGHLY CONFIDENTIAL – SOURCE CODE

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

HIGHLY CONFIDENTIAL – SOURCE CODE

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

EXHIBIT H TO CISCO'S OBJECTIONS AND RESPONSES TO ARISTA'S FIRST SET OF INTERROGATORIES

-74-

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]
 [REDACTED]
 [REDACTED]
 [REDACTED]
 [REDACTED]
 [REDACTED]

[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]
 [REDACTED]
 [REDACTED]
 [REDACTED]

HIGHLY CONFIDENTIAL – SOURCE CODE

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

HIGHLY CONFIDENTIAL – SOURCE CODE

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

A horizontal bar chart consisting of 25 black bars. The bars are arranged in a single column, with the longest bars in the middle and the shortest at the top and bottom. The bars represent a distribution of data, with the longest bars in the middle and the shortest at the top and bottom.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

HIGHLY CONFIDENTIAL – SOURCE CODE

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]
[REDACTED]

[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

EXHIBIT H TO CISCO'S OBJECTIONS AND RESPONSES TO ARISTA'S FIRST SET OF INTERROGATORIES

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]